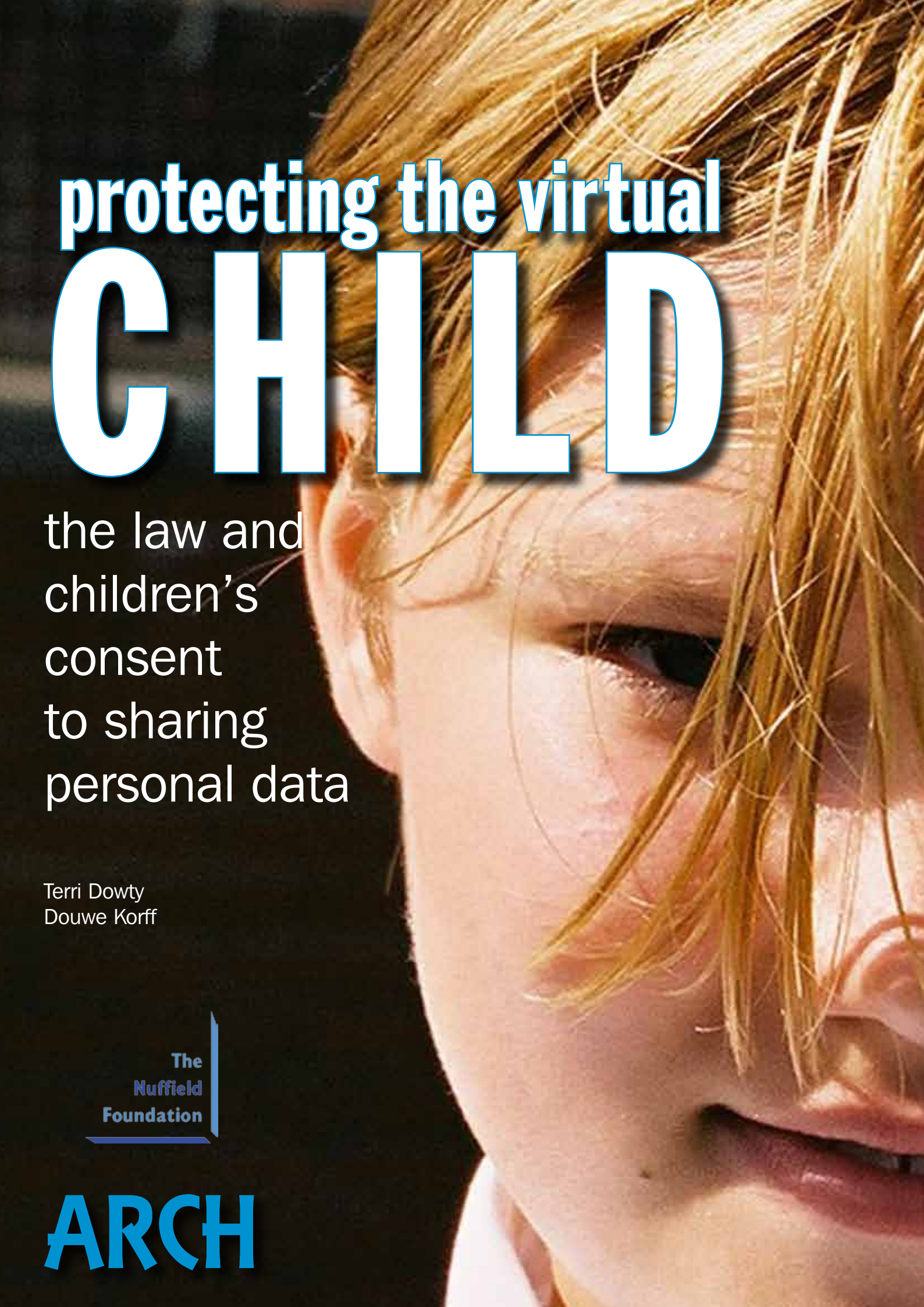


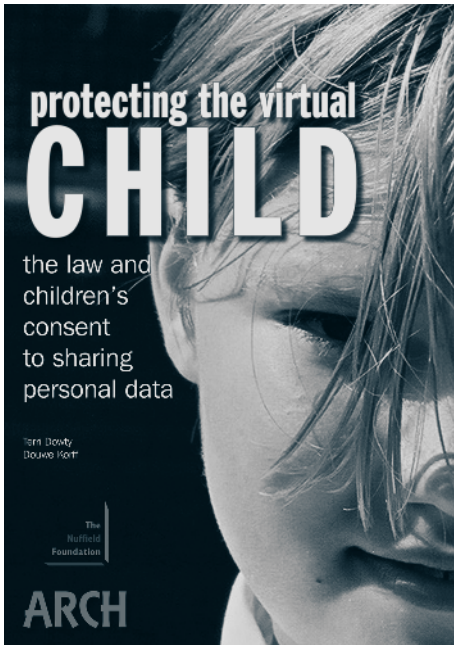
protecting the virtual CHILD

the law and children's consent to sharing personal data

Terri Dowty
Douwe Korff

The Nuffield Foundation

ARCH


protecting the virtual
CHILD
the law and children's consent to sharing personal data
Tom Doyle
Duncan Kerr
The Nuffield Foundation
ARCH

PROTECTING THE VIRTUAL CHILD:
THE LAW AND CHILDREN'S CONSENT TO SHARING PERSONAL DATA

Terri Dowty, Director of ARCH
Professor Douwe Korff
January 2009

ARCH

ARCH (Action on Rights for Children) is an organisation that works to promote children's civil rights. It has a particular interest in the effects of developments in Information Technology on children's rights to privacy and the protection of their personal data.

ARCH, 62 Wallwood Road, London E11 1AZ. Tel: 020 8558 9317. E-mail: archrights@arch-ed.org
Registered in England and Wales company number 5480579

The Nuffield Foundation

The Nuffield Foundation is a charitable trust established by Lord Nuffield. Its widest charitable object is 'the advancement of social well-being'. The Foundation has long had an interest in social welfare and has supported this project to stimulate public discussion and policy development. The views expressed are however those of the authors and not necessarily those of the Foundation

Acknowledgments

We should like to thank all the participants in this study, whose names and affiliations appear below. We initially approached ten academic and practising lawyers whom we knew by reputation from their work and publications on issues of children's consent. Seven of them responded positively and they, in turn, directed us to colleagues with similar expertise. We also met with staff from four specialist organisations. We are grateful to them all for giving us such generous quantities of their time and help. In particular, we should like to acknowledge Professor Jane Fortin, whose valuable advice at the outset of this project helped us to establish the parameters of our research.

We are grateful to Dr Ian Brown, Senior Research Fellow at the Oxford Internet Institute and a specialist in information security and networked systems, for providing us with expert advice on security practices within local authorities.

Our thanks also go to the Freedom of Information Officers and Children's Services staff in the 98 local authorities that responded to our requests for information; to Morag Driscoll, Director of the Scottish Child Law Centre; to Alex Dowty, a law undergraduate at Oriel College, Oxford, for the thorough research that he contributed to this project, and to Dr Eileen Munro, Reader in Social Policy at the London School of Economics, for her support, advice and helpful critiques of the various drafts.

Participants

Andrew Bainham: Reader in Family Law and Policy, Faculty of Law at the University of Cambridge and Fellow of Christ's College, Cambridge
Margaret Brazier: Professor of Law at the University of Manchester
Bev Clucas: Lecturer in Law at the University of Hull
John Eekelaar: Academic Director of Pembroke College, Oxford; Senior Fellow in Law 1965-2005
Lucinda Ferguson: University of Oxford lecturer in Family Law and Tutorial Fellow of Oriel College, Oxford
Jane Fortin: Professor of Law at the University of Sussex.
Jonathan Herring: Fellow of Exeter College, Oxford
Joan Loughrey: Senior Lecturer in Law at the University of Leeds
Aileen McColgan: Professor of Human Rights Law at King's College London and member of Matrix Chambers
Jean McHale: Professor of Law at the University of Leicester
Judith Masson: Professor of Socio-Legal Studies at the University of Bristol
Anne Morris: Senior Lecturer in Law at the University of Liverpool
Eve Piffaretti: partner in Morgan Cole, solicitors, specialising in health and social care law.
Joseph Savirimuthu: Lecturer in Law at the University of Liverpool
David Wolfe: member of Matrix Chambers, barrister specialising in public law
The British Medical Association
The Family Law Bar Association
The General Medical Council
The Information Commissioner's Office

Children and Consent

Executive Summary and Recommendations

1. The Government asserts in guidance that children in England can generally be presumed able to consent to the sharing of their personal and sensitive data from around the age of 12. Many local authorities repeat this advice. It has no basis in English law.

We recommend that reference to the age of 12 is removed from all guidance.

2. Children's competence to consent depends on their maturity; the quality of the information provided to them; the nature and sensitivity of the data; and the child's understanding of the purpose(s) for which the data are shared, the organisations or individuals who will have access to their data and the consequences of consent, or of failure to provide it. It requires careful assessment of each individual child.

We recommend that all local authorities are required to train practitioners in the assessment of children's capacity and competence to consent to information-sharing.

3. Parents have responsibility for their children. As a matter of good practice, arguably as a matter of law, they should be involved in the consent decisions of their competent children unless the child specifically objects, or there are special reasons against it.

We recommend that local authorities establish a default position of involving parents in decisions about sharing their children's sensitive data unless a competent child refuses such involvement.

4. When practitioners share a child's data, sensitive information may also be collected and shared about parents and siblings. The law already requires that parents should be made aware of this, subject to limited exceptions.

We recommend that this basic rule is followed in all cases, unless there are overriding reasons not to inform the parent.

5. Practitioners need sufficient knowledge of data protection to enable them to give children information in terms that a child can fully understand. The quality of information and training that local authorities give to practitioners varies significantly

We recommend that the Information Commissioner produces a code of practice for local authorities, setting out standards for data protection training and paying special attention to the protection of children's data.

6. The standard of training in information security given to practitioners varies widely. In some local authorities the inaccuracy of security advice and the inadequacy of security procedures give cause for concern.

We recommend that the Information Commissioner produces a code of practice setting out the minimum security standards for local authorities, and that local authorities ensure that all staff are trained in correct security procedures.

Introduction

The purpose of this report is to give an indication of current legal thinking on children's ability to give informed consent to information sharing, both in the UK and in other EU countries. It is divided into two sections: the first of these deals with the law in the UK; the second is a comparative study of seven EU countries undertaken for us by Professor Douwe Korff.

Since the UK Government published its green paper: 'Every Child Matters' in 2003, there has been a growing emphasis by Government on the need to share information about children across agencies in health, education, social care and youth justice in order to identify those children who may need services, or who are thought to be likely to develop problems in the future. This policy raises significant questions about who should consent to the sharing of that data. The Government has said that children from around the age of twelve are usually of sufficient maturity to consent in their own right.

Our UK research was aimed at establishing the legal basis for claims about children's capacity to consent to data-sharing. The subject is complex because it involves applying the existing body of law on the circumstances in which children can consent to specific services, such as medical treatment or legal representation, to the more abstract process of sharing personal data. No case specifically about children's consent to data-sharing has yet been before the courts and thus it is to a large extent uncharted territory.

We had a series of semi-structured interviews with fifteen academic and practising lawyers who have specific knowledge of consent issues, and with representatives of the Family Law Bar Association, the General Medical Council, the British Medical Association and the Information Commissioner's Office. The questions that we used to prompt discussion now form the headings in this report, and further details of our interviewees can be found in the acknowledgments.

We also sent requests via email to 126 local authorities for the information given to practitioners about information-sharing; the assessment of a child's competence to consent; data protection and information security. We received electronic replies from 94 of these local authorities. A further four replied by post, but because of the scale of the task we faced in scrutinising the information, we used only material that was supplied electronically.

The EU research was carried out by Professor Douwe Korff, an international lawyer and specialist in European data protection and human rights law. His comparative study of children's consent in 7 EU countries follows our examination of the position in the UK.

Throughout this report, our aim has been to write in a way that will make the subject readily understandable to non-lawyers, but we hope it will be helpful to lawyers and policy-makers in giving an indication of the areas of agreement and contention in the law relating to children's capacity to give informed consent to the sharing of their sensitive data.

Background

The idea that children under the age of 16 can on occasion give valid consent is not new. Over the years a body of law has developed that makes it clear that, in some circumstances, children can obtain information or services and make decisions on their own behalf, if necessary without the involvement or knowledge of their parents. Children can also exercise rights over their data to

the extent of forbidding others – including their parents – from having access to their confidential records.

It has long been the case that agencies can share information without consent about children whom they believe to be at risk of significant harm from neglect or abuse. It is also true that practitioners have always maintained case notes and discussed particular concerns with each other. However, what is relatively new is the question of whether children can consent to having sensitive data that they reveal to one person stored on a database and shared with others. In this instance, 'sensitive' means information about their mental or physical health, their beliefs and their private lives

The reason that this issue has come to the fore is that developments in Information Technology have made it possible to store large quantities of personal information about every child in easily accessible and potentially permanent records, and to share those records rapidly with other people. In the past, decisions about whether children can give valid consent have concerned single cases, usually in the medical or legal arena. Now, a child's entire education or health record could be despatched to another practitioner in less time than it would take to type the covering email. Information that would once have occupied a large room full of filing cabinets can be fitted on to a USB stick, or an entire database of 11 million records downloaded on to two CD-Roms – and a series of highly-publicised lapses in data-handling have made the consequent security vulnerabilities abundantly clear.

The sheer scale of what is now possible has allowed the development of entirely new government policies based on the monitoring of all children's progress through the sharing of information about them and their families between the practitioners who work with them across a range of agencies. Information-sharing, and the rules governing consent to that sharing, also have implications for the way companies do business with children. As the industry-based 'Children's Privacy Protection Network' points out:

> *'…children are increasingly becoming important economic actors, with significant purchasing power and distinct economic behaviour. With the availability of accessible technology, children are also interacting with the world around them in increasingly sophisticated ways, both with commercial organisations and peer to peer networks.'* [1]

Government policy and children's online activities raise all kinds of questions about confidentiality and the integrity of data, and they push the vital issue of who can or should consent to the collection, storage and sharing of children's confidential information to the top of the agenda.

In 2003 the government launched its 'Every Child Matters' agenda. It was conceived as a way of monitoring all children's welfare against five 'outcomes': that they should be healthy; stay safe; enjoy and achieve; make a positive contribution and achieve economic wellbeing. The achievement of these outcomes is seen as dependent on the 'joining-up' of services around each child, with the practitioners involved with a child collecting and sharing information. Much of this information is held on electronic systems, chiefly case management systems at local level that are built to a mandatory specification to ensure interoperability (the capacity to exchange data electronically), and the government is also constructing two national databases to act as a hub for the range of local systems.

Most people are now aware of the 'ContactPoint' database: a central index of all children in England containing basic information about every child plus the contact details of the practitioners working with them. Plans are also in train to introduce a second national database – known as the eCAF –

which is to hold the personal profiles of children seeking additional services over and above universal education and healthcare provision. This profiling is carried out under the 'Common Assessment Framework' (CAF), a standardised tool for the use of all practitioners except social workers, designed to gather and share assessment data about children and their families in order to provide services and spot early signs of problems that are thought to be predictive of poor outcomes such as criminality, teenage pregnancy or educational failure.

Where the sharing of such sensitive data is involved, the Data Protection Act 1998 requires that the specific consent of the person to whom the data refers (the 'data subject') should normally be obtained. This is where the problem addressed in this report begins: who is able to give this consent? Should it be the child or his parents – or both? It may be a clear-cut decision if the child is four years old, but what if he is fourteen? What if the data refers to a confidential service which the child has obtained perfectly legitimately without parental knowledge? What if it includes information about siblings and parents?

The Government has attempted to deal with what is a very confused and confusing area of law by advising in guidance that a child of around 12 is normally competent to consent to information-sharing:

> *'A child or young person, who has the capacity to understand and make their own decisions, may give (or refuse) consent to sharing ... Children aged 12 or over may generally be expected to have sufficient understanding.'* [2]

This assertion is apparently based on advice from the Information Commissioner and an interpretation of the decision of the House of Lords in *Gillick v. West Norfolk and Wisbech Area Health Authority*.[3] This case (to which we shall refer as '*Gillick*') gave rise to a concept known as the '*Gillick competent*' child and a set of rules known as the '*Fraser guidelines*'. It is important to note from the outset, though, that this case did not indicate any age whatsoever at which a child might be competent to give valid consent, nor did it proceed in any way upon that basis.

Development of the Law

Up until the second half of the 20th Century, decisions regarding children and young people who had not reached the age of majority were taken by their parents in the majority of cases. There gradually developed a body of law which recognised that children and young people could obtain medical treatment in certain circumstances without parental consent.

The Family Law Reform Act 1969 provided, in section 8, that a person aged 16 or over could, despite being a minor, consent to medical or dental treatment as though they were of full age.

At the beginning of the 1980s, *Gillick* of was one of the first to examine the ability of those under 16 to consent. Mrs Gillick sought a declaration from the court that it was unlawful for a doctor to prescribe contraception for a girl under 16 without the consent of her parents. She lost at first instance, won before the Court of Appeal and then lost again in the House of Lords.

In the House of Lords, Lord Fraser pointed out that the Court of Appeal, in finding for Mrs Gillick, relied heavily on an 1883 case, *'In re Agar-Ellis'*[4] which upheld a father's right to restrict communication between his daughter and her mother simply because that was what he desired rather than because there was any cause which would now be seen as reasonable.

Lord Fraser stated that this case had been *'much criticised in recent years and in my opinion with good reason'*, and went on to cite with approval a decision of Lord Denning MR in *Hewer v Bryant* [5]:

> *'I would get rid of the rule in* In re Agar-Ellis *and of the suggested exceptions to it. That case was decided in the year 1883. It reflects the attitude of a Victorian parent towards his children. He expected unquestioning obedience to his commands. If a son disobeyed, his father would cut him off with a shilling. If a daughter had an illegitimate child, he would turn her out of the house. His power only ceased when the child became 21. I decline to accept a view so much out of date. The common law can, and should, keep pace with the times. It should declare, in conformity with the recent Report of the Committee on the Age of Majority [Cmnd. 3342, 1967], that the legal right of a parent to the custody of a child ends at the 18th birthday: and even up till then, it is a dwindling right which the courts will hesitate to enforce against the wishes of the child, and the more so the older he is. It starts with a right of control and ends with little more than advice.'*

Lord Denning had anticipated the passing of the Family Law Reform Act 1969, s1 of which, when it came into force on 1st January 1970, lowered, in England and Wales, the age of majority from 21 to 18 years.

'*Gillick*' still provokes much discussion, but the key message of it is set out in the form of guidelines taken from Lord Fraser's speech, with which Lord Scarman and Lord Bridge specifically agreed, in which he set out the following criteria under which a doctor could lawfully provide contraception to an under 16 year old without being under a duty to inform her parents:

1) that the girl (although under 16 years of age) understands his advice;
2) that he cannot persuade her to inform her parents or to allow him to inform them that she is seeking contraceptive advice;
3) that she is very likely to begin or to continue having sexual intercourse with or without contraceptive treatment;
4) that unless she receives contraceptive advice or treatment her physical or mental health or both are likely to suffer;
5) that her best interests require him to give her contraceptive advice, treatment or both without parental consent.

These have become known as the *'Fraser guidelines'*; they are narrowly drawn and medically focussed. However, in order to understand the wider significance of Gillick, the speeches of both Lord Fraser and Lord Scarman, should be read in full. They are important to an appreciation of the basis of the sometimes conflicting views of lawyers on the subject of children's capacity to consent. They summarise previous developments in issues of children's consent, and present some persuasive opinion on the possible future direction of travel. However, whilst these give some indication of how they were thinking, it is important to note that their remarks are *'obiter'* – that is, they do not form part of their decision.

Indeed the *Gillick* case might be seen as the high-watermark of children's rights of consent and, in practice, its application has been rather erratic. The Court of Appeal resisted its full possible impact in 1991-92 by holding, in the cases of *Re R*[6] and *Re W,*[7] that although a young person's consent could enable a medical procedure to take place, this did not mean that refusal would prevent it. However, the idea of young people being involved in and consenting to that which affects them has grown in other areas, for example *Re S (Change of Surname)*[8] or *Re S (Specific Issue Order: Religion: Circumcision)*[9].

More interestingly for our purposes here, the question arose, in the case of *Re Roddy (A Child) (Identification: Restriction on Publication)*[10], of a young person[11] who was granted permission to divulge information about herself to a newspaper, where orders had already been made to protect the anonymity of both herself and other family members. This was justified by her right to freedom of expression. It would also seem that parents may not necessarily consent to disclosure on behalf of their child. In *Re Z (A Minor) (Identification: Restrictions on Publication)*[12] a mother wished to have a documentary made about the treatment her child had received. She was prohibited from doing so as it was not in her child's interests. In *Clayton v. Clayton*[13] a father was prohibited from making a film involving his child as she was not yet competent to make her own decision about participating in it.

It is not our intention in this study to do more than touch on some of the more important cases since *Gillick*. None has covered scenarios comparable to the emerging issues surrounding a young person consenting to the sharing of sensitive personal information.

Importantly since the decision in '*Gillick*' the Children Act 1989 has enshrined the principle that the welfare of the child is *'the court's paramount consideration'*[14], and the Human Rights Act 1998 has introduced consideration of the European Convention on Human Rights. In addition, although it has not been formally made part of domestic law, the courts are increasingly referring to the United Nations Convention on the Rights of the Child, which the UK ratified in 1991.

These provisions, together with the Data Protection Act 1998 itself, have all played their part in the growing awareness that children can and should be consulted and make decisions in matters that affect them, thereby significantly affecting children's rights to confidentiality, to have their views considered and to give consent.

In 2006, twenty years after *Gillick*, a remarkably similar case came before the courts: *Axon v. The Secretary of State for Health*[15] concerned the application of Mrs Sue Axon that she should be informed if her underage daughter should seek termination of a pregnancy. Dismissing her application, Silber, J effectively reiterated the guidelines given by Lord Fraser, and said:

> *'I have concluded that Gillick remains good law'.*

How are we to understand the significance of Gillick?

We were initially baffled by the spectrum of views on the interpretation of *Gillick* expressed by the lawyers whom we interviewed in the course of this study. David Wolfe assisted us by pointing out there is no categorical answer to the question of whether a child can give consent to information-sharing; what we were hearing was a selection of opinions and 'best theories' that would be argued if a case were to come before the courts.

The *Gillick* case was highly controversial, attracting wide publicity and anguished debate. In the court of first instance, Woolf, J dismissed the action, in which Mrs Gillick had sought to forbid the provision of contraceptive advice to her underage daughters without her knowledge or consent. The Court of Appeal subsequently overturned that decision. When the appeal finally reached the House of Lords, two of the five Law Lords dissented, and of the remaining three, Lord Fraser and Lord Scarman appeared at times to be arguing from different premises.

Both Lord Fraser and Lord Scarman explicitly agreed with the comments of Lord Denning in the case

of *Hewer v. Bryant* (see above). Lord Fraser said that when advising a minor about contraception, a doctor should:

> *'.. always seek to persuade her to tell her parents that she is seeking contraceptive advice, and the nature of the advice that she receives. At least he should seek to persuade her to agree to the doctor's informing the parents.'*

He added:

> *'Once the rule of the parents' absolute authority over minor children is abandoned, the solution to the problem in this appeal can no longer be found by referring to rigid parental rights at any particular age. The solution depends upon a judgment of what is best for the welfare of the particular child. Nobody doubts, certainly I do not doubt, that in the overwhelming majority of cases the best judges of a child's welfare are his or her parents.'*

Lord Scarman did not put forward any test of welfare, but focused on whether the child has capacity:

> *'I would hold that as a matter of law the parental right to determine whether or not their minor child below the age of 16 will have medical treatment terminates if and when the child achieves a sufficient understanding and intelligence to enable him or her to understand fully what is proposed. It will be a question of fact whether a child seeking advice has sufficient understanding of what is involved to give a consent valid in law.'*

It is reasonable to say that amongst the obiter remarks one can find support for a variety of arguments, and the position has been further complicated by subsequent developments in jurisprudence in the related area of confidentiality, in the law of contract, by the Children Act 1989 and by legislation on human rights and data protection.

Bev Clucas suggested that *Gillick* gave rise to five possible interpretations. The strongest of these is that it affirms or establishes the idea that a child's right to self-determination has to be respected when they acquire sufficient capacity.

The next level is that *Gillick* affirms, or establishes, the idea that a child's right to self-determination should be respected when they have capacity to make a particular decision, but the issue of contraceptive treatment requires a particularly high level of understanding and intelligence.

The third position is that one must respect self-determination when the child has sufficient capacity on a factual issue, the child refuses parental involvement and the procedure is in the child's best interests.

All three of these interpretations are capacity-related and mention self-determination, but they qualify it in different ways. While the first two rely on capacity, the third, at least in relation to contraceptive treatment, has an additional hurdle of best interests.

The fourth interpretation emphasises the medical practitioner's assessment of the child's best interests rather than the exercise of autonomy by the child. If a child is sufficiently mature, the courts are prepared to accept the judgment of the medical practitioner as to the child's best interests.

The fifth position is that *Gillick* is purely a legal shield for doctors, intended as a means of ensuring that medical treatment is lawful, and that the practitioner is not liable for assault.

John Eekelaar, Lucinda Ferguson and Jonathan Herring were clear that *Gillick* established a common law principle in the matter of young people's consent generally. David Wolfe and Aileen McColgan believe that it is questionable whether *Gillick* can be mapped onto the largely abstract and intellectual matter of information-sharing. In Margaret Brazier's view:

> *'It's an exceptionally difficult case to answer because the jurisprudence is not concerned with data sharing – it's about taking the pill or being touched by a doctor in a way that would otherwise be an assault. I can see that one could argue that data sharing is of a different order to a blood transfusion, although I have not seen that case made anywhere.'*

The question of children's consent to data-sharing takes us into as yet uncharted waters. Should it be easier or harder for a child to consent? It brings into sharp relief the tensions between parental responsibility and the child's evolving capacity; between the child's increasing autonomy and their need for guidance and protection. Parents need knowledge about what is happening in their children's lives in order to exercise the parental responsibility required of them by the Children Act 1989, but children sometimes need to talk in confidence to practitioners. They have rights to confidentiality and privacy – but so, too, do their parents and siblings. It does not advance the recognition of children's human rights if they are widely seen as a source of conflict between child and parent, and so a satisfactory balance needs to be found that addresses the many different issues that arise in this new age of accessible records, rapid information-sharing and joined-up government.

Given the range of possibilities, none of which considers the position by reference to a specific age under 16 at which there is a presumption of competence, it must be asked how the Government in guidance is able to state that: *'children aged 12 or over may generally be expected to have sufficient understanding'*.

Can a 12-year-old consent to having their sensitive data shared?

One of the points on which most of our interviewees agreed is that in England, Wales and Northern Ireland, there is no scope for presumption of a child's competence at any fixed age. Margaret Brazier pointed to the ordinary rules that you cannot make any assumptions about a person under 16; Aileen McColgan reflected the opinion of the majority in saying that, while there is a vast spectrum of competency and development across any age group, adolescence is a time of rapid changes and by its nature a time during which the characteristics of child and adult are mixed, often in unpredictable ways. Two children or teenagers of the same age will often vary wildly in competence and maturity.

Several interviewees said that if it were essential to prescribe an age, they would have serious reservations as to whether it should be 12; their suggestions ranged from 13 to 15. The General Medical Council said that those respondents to a consultation exercise who were keen to have a guideline figure tended to favour 13. The British Medical Association thought that a presumption of 12 might be acceptable with some caveats about the relative seriousness of the information, and the need to take developmental issues into account.

Anne Morris highlighted an interesting problem in fixing any age: a far younger child might be

competent to consent in some circumstances. Giving an age for a presumption of competence may deter practitioners from considering this possibility and preclude younger children from making decisions that are within their capabilities, which would not conform to the principles set out in *Gillick*, based as they are on assessment of the individual capacity of each child.

Gillick did not prescribe an age at which a child could be presumed competent to consent to contraceptive treatment, nor did it suggest any age at which it might be appropriate to assess such competence. In his speech, Lord Scarman warned:

> *'Certainty is always an advantage in the law, and in some branches of the law it is a necessity. But it brings with it an inflexibility and a rigidity which in some branches of the law can obstruct justice, impede the law's development, and stamp upon the law the mark of obsolescence where what is needed is the capacity for development. The law relating to parent and child is concerned with the problems of the growth and maturity of the human personality. If the law should impose upon the process of "growing up" fixed limits where nature knows only a continuous process, the price would be artificiality and a lack of realism in an area where the law must be sensitive to human development and social change.'*

The Family Law Bar Association (FLBA) expressed their concern that the mere mention of an age, at which competence to consent might be assessed, is all too easily eroded into a *de facto* 'age of consent'. We have seen a great deal of evidence that this concern is well founded. To give some examples, advice issued to schools by Bristol Children & Young People's Services on consent to the supply of information to the Connexions Service says:

> *'Pupils aged 12 and above, need to be reminded that they are deemed mature enough to act independently of their parents' wishes in this area.'*[16]

The Information Sharing Protocol for Wolverhampton says:

> *'If the client is aged less than 12, a legal guardian may provide written consent on her/his behalf (preferably in the presence of the child/young person wherever possible). If the client is aged 12 or over and has a condition that precludes her/him from signing a consent form, a legal guardian may act on her/his behalf.'* [17]

They are certainly not alone in asserting that competence can be assumed from the age of 12. We have seen similar statements in other material supplied to us by local authorities. There appears to be considerable variation around the country in the advice given on the law relating to consent. Some local authorities provide practitioners with information that does not mention a specific age and makes it clear that competence must be assessed on a case-by-case basis. However, most local authorities advise that the age of 12 is one at which competence is likely. One or two go further by saying that, *'a child of or over the age of 12 years shall be considered to have legal capacity'*. Some appear to believe that the age of 12 is mandated by the Department for Children, Schools and Families or by the Data Protection Act 1998; in one case, a local authority says that it was established directly by the *Gillick* case itself.

Recognising that the area of consent is difficult, one local authority offers practitioners the following reassurance:

> *'Practitioners may find themselves in court for a number of reasons during the course of their career for example as a witness in a civil or criminal prosecution. It is highly unlikely that they will find themselves in court as a result of sharing information and in that event would be fully*

supported by managers if they have followed agency procedures.'

This would seem to be scant comfort for the practitioner who is at the sharp end of a court case as a result of confusing or inaccurate advice.

We have not been able to find any precedent or authority in the Common Law or statute which asserts a *presumption* that a child of 12 is competent to consent and in general terms it is certain that such a child does not have legal capacity.

In considering how such an age has been arrived at in the Government's and in the Information Commissioner's guidance, it may be useful first to consider the position, both historically and now, in Scotland.

It should from the outset be borne in mind that the legal system of Scotland, which is based on Roman law, has developed entirely separately from the Common Law jurisdiction of England, Wales and Northern Ireland.

In Scotland prior to 1991, girls reaching the age of 12, and boys the age of 14, achieved the legal status of 'minority', which made it possible for them in certain circumstances to enter into legally-binding contracts. (In England, Wales and Northern Ireland, with certain exceptions, including employment, such legal capacity is not attained until the young person becomes 18.)

In order to rationalise and restrict the legal capacity of both boys and girls under 16 in Scotland, the Age of Legal Capacity (Scotland) Act 1991 was introduced as a Private Member's Bill with cross-party support. Lord Macaulay of Bragar explained upon the introduction of the Bill into the House of Lords, that:

'...the intention behind the Bill is to replace what is an extremely complex system with a more rational and simplified two-tier system. Under the Bills' provisions, which I outlined earlier, young people under the age of 16 will in general have no legal capacity, subject to certain specific exceptions; for example, the right to make a will and the right to consent to medical treatment. Those young people of 16 and 17 years of age will have full legal capacity to enter into binding transactions but, as a protection against their relative immaturity, they will enjoy the limited protection of being able, before they reach the age of 21 years, to seek a court order to set aside transactions which, in terms of the legislation, are prejudicial to them.' [18]

The Age of Legal Capacity (Scotland) Act 1991[19] provides as follows:

1 Age of legal capacity
(1) As from the commencement of this Act–

(a) a person under the age of 16 years shall, subject to section 2 below, have no legal capacity to enter into any transaction[20]*;*

(b) a person of or over the age of 16 years shall have legal capacity to enter into any transaction...

2 Exceptions to general rule
(1) A person under the age of 16 years shall have legal capacity to enter into a transaction–

(a) of a kind commonly entered into by persons of his age and circumstances, and

(b) on terms which are not unreasonable.

(2) A person of or over the age of 12 years shall have testamentary capacity, including legal capacity to exercise by testamentary writing any power of appointment.

(3) A person of or over the age of 12 years shall have legal capacity to consent to the making of an adoption order in relation to him; and accordingly etc...

(4) A person under the age of 16 years shall have legal capacity to consent on his own behalf to any surgical, medical or dental procedure or treatment where, in the opinion of a qualified medical practitioner attending him, he is capable of understanding the nature and possible consequences of the procedure or treatment.

(5) Any transaction-

(a) which a person under the age of 16 years purports to enter into after the commencement of this Act, and

(b) in relation to which that person does not have legal capacity by virtue of this section,

shall be void.

We have been advised by the Scottish Children's Law Centre and by the General Medical Council (GMC) that the Act does not relieve a practitioner of responsibility for assessing the competence of a person under 16, but the mention of the age of 12 is indicative that it is from this age that competence might be presumed.

Section 66 of The Data Protection Act 1998[21] specifically addresses the position in Scotland:

Exercise of rights in Scotland by children

(1) Where a question falls to be determined in Scotland as to the legal capacity of a person under the age of sixteen years to exercise any right conferred by any provision of this Act, that person shall be taken to have that capacity where he has a general understanding of what it means to exercise that right.

(2) Without prejudice to the generality of subsection (1), a person of twelve years of age or more shall be presumed to be of sufficient age and maturity to have such understanding as is mentioned in that subsection.

The Information Commissioner's guidance[22] to the Data Protection Act 1998 addresses s.66 in the following terms:

4.1.6 ...The position in England, Wales and Northern Ireland is unchanged with the Act but section 66 of the Act brings the position in Scotland into line with the rest in that it provides that a person under 16 may exercise any right under the Act when he has a general understanding of what it means to exercise that right and that a person of 12 years or more

shall be presumed to be of sufficient age and maturity to have such understanding.

The wording of this paragraph is rather confusing. It states that the purpose of s66 is to bring Scotland into line with England, Wales and Northern Ireland by presuming that a child of 12 has the competence stated, yet it would appear that in 1998 when the Data Protection Act was enacted, it is only in Scotland, following the passing of the Age of Legal Capacity (Scotland) Act 1991, that such a presumption can be said to exist. As we have stated, we can find no authority for the existence of such a presumption in England, Wales and Northern Ireland.

While it is true to say that, following *Gillick*, if its principles extend beyond medical matters, children under 16 in England and Wales may be able to exercise some rights without parental consent when they are sufficiently mature, there is in our view no basis for saying that the age of 12 has significance other than in Scotland. When we discussed the matter with a member of the Information Commissioner's staff, we were told that the salient factor is that of when a child becomes capable and:

'Our view is that around 12 children become more mature, but that could happen sooner or later. We picked 12 as a rule of thumb, but are sorry we had to do so.'

It also needs to be borne in mind that, as several of our interviewees explained, a child's competence to consent will inevitably relate to the complexity of the decision to be taken. In the medical context, a child may be competent to consent to a course of antibiotics or to have a sprained ankle bandaged, but that same child may not be capable of consenting to treatment that has potentially serious side-effects or long-term implications.

A child of 12 – and quite conceivably younger – may well be capable of exercising subject access rights under the Data Protection Act 1998 to see the information that is held on him and to forbid its disclosure to others. The General Medical Council suggested to us that if a child can prevent disclosure, then that implies he can also consent to disclosure. However, there is a difference between accessing one's records or issuing an instruction that maintains the status quo of confidentiality, and taking an active decision to release information that may have long-term consequences. John Eekelaar points out that information sharing is a more complex issue than subject access, while Joan Loughrey says:

'Choosing to have your confidentiality breached is much more of an autonomy right. You need to have the capacity to make an autonomous decision regarding the release of information.'

Although practitioners and local authorities would undoubtedly prefer to have the ambiguity of the current legal position resolved, in Andrew Bainham's opinion this is properly a matter for parliament:

'Gillick was expressly against drawing rigid lines like this although legislation does of course fix ages for such matters as sexual activity, employment, leaving school and so on. The point here is that this is for parliament and not for the government just to pluck this age out of the air. Where legislation governs a specific activity Gillick does not apply and it would of course be open to parliament to exclude the operation of Gillick from this area entirely by legislating. But until it does so the common law and Gillick apply and I reject the notion that there is any magic in the age of 12.'

His view echoes that of Lord Scarman in *Gillick*:

> *If certainty be thought desirable, it is better that the rigid demarcations necessary to achieve it should be laid down by legislation after a full consideration of all the relevant factors than by the courts confined as they are by the forensic process to the evidence adduced by the parties and to whatever may properly fall within the judicial notice of judges.*

The elements of competence

To say that competence cannot be presumed at any specific age is not in any way to imply that a person under 16 could never offer valid consent to the sharing of their personal data, or that a child of 12 – or younger – may not be competent to consent to certain things. This is a point that needs to be stressed because it is something on which all of our interviewees were perfectly clear. As Lucinda Ferguson explained:

> *'Lord Scarman set out the general principle in Gillick, and Lord Fraser set out specific requirements for cases of that type.'*

However, the child has to meet the *Gillick* criteria and, once any possibility of a 'rubber-stamp' decision based on age has been removed, it becomes necessary for practitioners to engage in a far more subtle process of information-giving, checking and assessment.

Competence is not a fixed state that a child attains: it is issue-specific and relates to the nature of the information and the gravity of the decision. Several interviewees stressed that context is important. The FLBA, for example, said that decision-making is:

> *'…down to the competence and intellectual capacity of the individual child to understand the proceedings and the nature of how their wishes and feelings will be utilised, and whether they understand their own situation.'*

A child needs to be given sufficient information about the implications of the proposed course of action to weigh up the relative risks and benefits in order to reach a decision. John Eekelaar says that:

> *'If it was involving adults it would need to be rigorous and clear. Children need to be approached in the same way, they are perfectly capable and they need the same information. It's not an exact match because it involves children, but it is similar.'*

Eve Piffaretti believes that consent is about more than simply being given information:

> *'Clients focus on informed consent, but I say valid consent because you must have capacity, be informed and it must be voluntary. Also, consent to what? In medical it is a specific treatment with specific consequences. With ContactPoint you have information and possible consequences.'*

Competence will depend upon the individual child's maturity, intelligence and understanding in relation to the particular decision. Lucinda Ferguson emphasises that this is not simply an issue of cognitive capacity, pointing out that in judgments concerning a child's refusal of consent to medical procedures, courts tend to talk about psycho-social maturity, not cognitive understanding. Margaret Brazier agrees:

'Gillick is talking exactly about psycho-social maturity. A person under 16 must have maturity and intelligence. We don't apply intelligence over 16. It's a clear indication that they're looking for a level of psycho-social maturity.'

Do parents need to be involved?

This question provoked a wide range of thoughtful responses across a full spectrum of views. Because of the many different issues that our interviewees raise, we quote extensively from them below.

The point of *Gillick* was that it allowed an under-age girl to receive contraception without the knowledge or involvement of her parents. As we have already explained, there is disagreement amongst lawyers as to how *Gillick* should be applied. One of the key questions is how far parents need to be involved.

Lord Fraser established a default position that parents should ordinarily be consulted or at least informed when a girl under 16 sought contraception; it is for the child to indicate that she does not want parental involvement. Whether that default applies beyond the specific circumstances that were then under consideration will depend to some extent on one's interpretation of the judgment. Lord Scarman, on the other hand, made no mention of parents when he said that the important factor was one of the child's own capacity.

Another factor in the consideration of the role of parents is the concept of 'parental responsibility', defined in the Children Act 1989 as giving them:

'…all the rights, duties, powers, responsibilities and authority which by law a parent of a child has in relation to the child and his property.' [23]

Aileen McColgan questions whether the exclusion of parents from decisions ordinarily needs to be considered. She says that Gillick provides guidance in cases where a teenager is unwilling or unable to talk to her parents about contraception or the parents would be opposed to such provision; it is based on a situation where the girl herself has stated that she does not want her parents involved. There is thus a conflict between the view of the girl and the view of her parent as to medical treatment she seeks. In the case of data sharing in the context of the 'Every Child Matters' agenda, there may be no reason for such conflict to exist and thus no need to differentiate between child and parents in this way.

The BMA's view is that it is good practice to include parents, depending on the child's view and the doctor's assessment of their competence:

'If the young person is competent, I would say they could proceed, but it would be good practice to involve the parents if the child is content to. If they are competent the doctor is not under an obligation to involve them. What Fraser said specifically relates to sexual activity, which he separates off discretely. It's clear you could legally take that position apart, but the same goes for the alternative. There is no consensus at all.'

Joan Loughrey's opinion is that if the child is competent, parental involvement is not necessary in order for the consent to be valid. She also points out:

> *'The courts are sympathetic to authorities' requests to use information. It would need to be quite egregious to cause them to intervene. The authority is using the information and it is going towards the child's welfare.'*

Jonathan Herring suggested that there may be good reason for a child not to want a parent to be informed, for example in the case of young carer, and Andrew Bainham said that:

> *'If the child is in a dysfunctional family, or where the child has been abused, neglected or has left the parental home, there may be good reasons why the parents ought not to be informed and indeed some cases in which it would be dangerous to inform the parent. The same goes for data relating to sensitive sexual issues. But I think it would be for the professional concerned to make this evaluation and decide whether or not it would be appropriate to press the competent child to consult the parents.'*

In Lucinda Ferguson's view, because *Gillick* recognises that there are situations where children don't need an adult, it ought to be feasible not to involve them. John Eekelaar agrees, but adds:

> *'It seems to me that a child with a difficult choice should have the right to the resources to be informed, whether that is a parent or someone else. They have the right to act freely in an informed way. If one is not permitted to go away and consider one's options then one is not acting freely.'*

The FLBA echoes this concern, saying that the child may give a good reason as to why the parents should not be involved, but otherwise why should children have the burden of the decision on their own? They point out that adults often want to speak with others when they are faced with a decision, and a presumption that children should be making these decisions in isolation robs them of backup and support.

The Information Commissioner says that:

> *'Where personal data, electronic capture, is concerned, although it may be administrative and not entirely Data Protection, it is best practice to involve parents, but a practitioner is not legally required to do so.'*

Eve Piffaretti advises clients that as a matter of good practice they should try to involve parents unless the child is adamant, in which case confidentiality should be maintained unless there is a child protection need to over-ride the child's decision. Jane Fortin agrees that it is good practice to involve parents rather than a matter of law, and in Judith Masson's view:

> *'I don't think you need to involve the parent. You can as good practice, and it's unclear if you need to…as a society we don't necessarily accept that parents not knowing is a good thing, but we have to balance that against the consequences of not respecting the confidentiality of mature minors.'*

Bev Clucas suggests:

> *'The reason that a doctor wouldn't need to inform parents is because he's independent and concerned with best interests, with no other agenda. So, without saying that a parent has to be involved in everything, I would say they should unless the person seeking the consent was independent with no other agenda.'*

Margaret Brazier says that if you take the analogy with treatment, there is no requirement to involve parents when dealing with a competent minor. However, she adds that statements about parents can be looked at in two contexts:

> *'First, if a young person, making a decision of gravity and consequence, refuses to involve their parents that may give an indication that they are not mature enough to be competent. Secondly, any doctor has a duty to respect their patient's wishes, but also to act in their best interests. Even if the young person is competent it may still be in their best interests to involve the parents, who might have useful information. They are also likely to find out, and a rupture in the family would not be good for the child. Fraser was right to stress it.'*

In the FLBA's opinion, as a matter of law the proper approach is a presumption of parental involvement because they have parental responsibility, and government guidance saying that a child can be presumed able to give consent does not fit with that concept. They accept that in some circumstances there are difficult ethical issues about confidentiality, but point out:

> *'There is a great tension where the Government says that parents should take responsibility for criminal matters. If you have information relevant to that and the parents are not involved, then the parents are in the hot seat all of a sudden without having been notified to begin with. You can't have it both ways: parents are liable when something goes wrong, but not involved when they are trying to do something about it.'*

The same argument might also be applied to educational issues. The Information Commissioner says that many schools divide educational and pastoral records because parents have an absolute right to access a child's educational record, but the same is not true of personal information. We are not entirely convinced that problems can always be so neatly separated: a personal problem may directly affect school work, or be aggravated by anxiety about educational matters.

Andrew Bainham shares the FLBA's view that it is a matter of law to involve parents and that *Gillick*:

> *'...does not support a view that they can simply be routinely by-passed. It rather supports a form of participatory decision-making in which it would be normal to try to persuade a child to inform parents and bring them into important decisions. Cases subsequent to Gillick have made the important point that parents retain their parental responsibility until the child attains majority at 18 and this is so whether or not the child has capacity for decision-making. In other words, children's capacities and parental responsibility co-exist or are concurrent.'*

Joseph Savirimuthu points out that:

> *'Just because the child has rights doesn't mean there is no parental role. There is one of oversight. That is a distinction that is sometimes lost. The exercise of rights can be subject to oversight.'*

Anne Morris agrees:

> *'Post-Gillick and the Children Act 1989 there has been a tendency to stress autonomy. The problem is that until 18 it is part of parental responsibility to guide children in the use of their autonomy'*

Judith Masson says that it will depend upon what one thinks parental responsibility is for:

> *'With a non-Gillick competent child parents hold all the rights. The law is not clear if parental responsibility is for parents or for parents to look after the child, and you can construe the cases either way. In the cases, are parents consenting for their own need for services or on behalf of the child?'*

Information that children give may not only be personal to them: the Common Assessment Framework (CAF) is intended to be a 'holistic' assessment tool and, as such, includes questions about the child's family and relationships. The CAF practitioner guidance stresses that it should be indicated where a child is giving an opinion rather than a statement of fact:

> *'Opinions should be recorded and marked accordingly (for example 'Michael said he thinks his dad is an alcoholic').'* [24]

While it is important that a child can express anxieties to a practitioner who is trying to help, unless there are child protection concerns, should information or opinion about others be recorded and shared without the consent of the person to whom it refers? Anne Morris does not think that such information belongs to the child, while Joan Loughrey says:

> *'Interventions can invade a family and there must be parental rights. If information impacts upon family life, you have to tell them about it.'*

Jean McHale expresses uneasiness about the decision being taken away from parents because information may be harmful if it is shared. While the child should certainly have input into the decision, she questions whether it should be the sole decision of the child. She also raises the point that obtaining consent to disclosure from the child alone has implications across divergent religious and cultural groups within the UK that may engage Article 9 (freedom of thought, conscience and religion) of the European Convention on Human Rights:

> *'Here surely there will also be considerations of respect for freedom of religion, conscience and belief in relation to Article 9. Research undertaken with different cultural groups is likely to reveal very different attitudes in relation to the consent process depending on the nature of family relationships. This is something which does warrant further research and detailed examination.'*

If the child's consent is being sought about a minor issue to which, but for the cultural or religious views of the parents, children might be thought capable of consenting, should her consent be taken without reference to her parents, even though that might provoke friction in the family?

The different views outlined above demonstrate that parental involvement is a vexed question. Those whom we interviewed raise a variety of issues that need to be considered and it is clear from their sometimes sharply conflicting opinions that there is presently not a consensus on whether parents normally need to be involved in the decision to share the data of their competent underage children – nor, if they do, whether this is a matter of law or of good practice.

Our next set of questions was concerned with the level of knowledge and skill that a practitioner would need in order to assess a child's competence to consent, and the type of information that a child would need in order to make a properly informed decision.

The pre-conditions to seeking a child's consent

The Government has published information-sharing guidance which includes the following advice on seeking a child's consent:

> *3.23 Children aged 12 or over may generally be expected to have sufficient understanding. Younger children may also have sufficient understanding. As explained in paragraph 3.30, this is presumed in law for young people aged 16 and older. When assessing a child's understanding you should explain the issues to the child in a way that is suitable for their age, language and likely understanding. Where applicable, you should use their preferred mode of communication.*
>
> *3.24 The following criteria should be considered in assessing whether a particular child or young person on a particular occasion has sufficient understanding to consent, or to refuse consent, to sharing of information about them:*
>
> *Can the child or young person understand the question being asked of them?*
>
> *Do they have a reasonable understanding of:*
> - *what information might be shared;*
> - *the main reason or reasons for sharing the information; and*
> - *the implications of sharing that information, and of not sharing it?*
>
> *Can they:*
> - *appreciate and consider the alternative courses of action open to them;*
> - *weigh up one aspect of the situation against another;*
> - *express a clear personal view on the matter, as distinct from repeating what someone else thinks they should do; and*
> - *be reasonably consistent in their view on the matter, or are they constantly changing their mind?*
>
> *3.25 Considerations about whether a child has sufficient understanding are often referred to as Fraser guidelines, although these were formulated with reference to contraception and contain specific considerations not included above.*[25]

If reference to any expectation about the age of 12 is removed, this is a reasonable and brief summary of the factors that a practitioner should consider. However, it is only a summary and does not go into any detail about the way that the assessment should actually be conducted. Many local authorities appear to be relying on this section of guidance as providing adequate advice for practitioners, and our next question was designed to tease out whether the process requires a level of skill and training.

Does the practitioner need any specific training in how to assess a child's competence to consent?

There were mixed feelings amongst our interviewees as to the level of training – if any – that a practitioner needs in order to assess whether a child is *Gillick competent*.

The BMA believes there does need to be special training:

> *'It's very complex, the Mental Capacity Act 2005 gives pointers, but it's enigmatic, especially when it's on the threshold. One also needs to consider enrolling experts, those with expertise in consent involving young people. If you were to ask for the evidence base of competence decisions, it's often just gut decisions. It's always the thresholds that are troubling. I don't think people know what competence is, or its components. Memory is one, analytical capacity, cognitive linking. People need to know what they are looking at and for.'*

The GMC says that the issue is rather confused: the reality is that people have to make these decisions without particularly specific training, but whether they should or not is another matter. Eve Piffaretti, who gives training on consent, warns that you cannot take it as given that even very experienced healthcare professionals know how to assess competence.

In Anne Morris's view, assessment of competence does not involve particular expertise. The general test is sufficient understanding, maturity and intelligence, and if the assessor is provided with a list of risks and benefits, they should be able to gauge understanding. Margaret Brazier does not think that there is any prescribed set of skills:

> *'My immediate answer is that the case law does not require a qualification in assessing competence. The cases do seem to involve medical professionals, but I can't see a case for saying only clinicians can take consent.'*

Jane Fortin believes that *'ideally'* practitioners should be trained and Jean McHale says that training is necessary for the process to operate effectively. While Joan Loughrey is not sure that training is necessarily required as a matter of law, she points out:

> *'Findings in relation to competence, about confidentiality in withholding information about potential anorexia, are very inconsistent. If doctors are making mistakes, people less well-trained are more likely to do so...You need to think about training people to communicate in a way which is suitable to age, language and understanding. It needs, ideally, to be a lot more detailed. The ability to consider alternatives does form part of the test in Mabon.*[26] *Weighing things up is part of the adult test. The government guidance just sets it out – it doesn't tell you how to do it.'*

The strongest reaction came from the FLBA, whose members gave an immediate and unanimous reply that training is essential both in competence and more generally in capacity, the more so if consent is being sought from a child who has social or emotional difficulties. When we asked whether they would consider a hand-out or a single training session to be sufficient, they replied that it would *'almost certainly not'*, warning that, *'there is a lot of skill required to do this effectively'*.

Do local authorities offer training?

We asked local authorities to provide us with any information that they give to practitioners on the assessment of a child's competence to consent. We are treating the replies with a degree of caution because they were not always clear, and it may be that more training is offered than the material suggests. Some did not answer this section of our request, while others supplied somewhat irrelevant material without explanation. Several did not appear to understand the question and simply gave the circular reply that practitioners assess children according to the Fraser guidelines, without actually explaining whether, or how, they learned to do this.

Of the 94 replies we received, only four local authorities appeared to offer specific and ongoing training in assessing competence. A further two said that practitioners undertake an e-learning module on information-sharing that includes issues of consent. Eight said either that they did not offer any training or that social workers receive such training in the course of professional qualification, without mentioning any provision for other practitioners. The overwhelming majority relied on pointing practitioners to the section of government guidance quoted above or to very similar material.

What information does the child need if consent is to be 'informed'?

In the Information Commissioner's view, a child needs to know exactly what information is being talked about and what will be shared in as much detail as possible. They must be told with whom it will be shared and why, what the people receiving it will do, and how long it will be held for:

> *'We are adamant that consent is linked to Fair Processing. It's not just what the information is but what the consequences of sharing or not sharing might be. When talking to a child, it's not just 'can we share with this person for this', but the difficulties which might arise either way – that some people who see it may for example have to tell teachers or parents.'*

The Information Commissioner would like to see layered Fair Processing Notices: layer 1 giving basic information including where to obtain more details; layer 2 including legislative and/or practical reasons; layer 3 containing all possible information that a data subject might want. It should be borne in mind that if a child cannot understand a Fair Processing Notice, it may indicate that he is non-competent.

Judith Masson does not think that the child needs very much information because practitioners are presumably sharing it in the child's best interests. However, Jane Fortin says that the child should know the full implications of sharing the information, including the possibility that it may be lost or seen by unauthorised persons, and also the benefits of sharing it. Jean McHale agrees:

> *'The child should be informed as to why the information was being sought, where it would be held and also informed as to the consequences of the retention of this data – some of which may be adverse. Practitioners should be aware of the Data Protection Act, the need for security of the relevant data and the security policy within the local authority.'*

David Wolfe and Aileen McColgan both say that it is crucial that people are made aware of the purposes for which the information will be used. They must be informed about the security of their data and the potential risks to that security. Bev Clucas suggests that, since *Gillick* was clear that there was a need to understand the social and moral considerations, children should be aware of the arguments for and against information sharing.

In the GMC's view, it is important that children are given sufficient information to make a decision:

> *'The question is if the person is able to use, retain and weigh the information. Some considerations are specific to information sharing. They must understand the nature, purpose and consequences of disclosure and non-disclosure. We talk about making sure the person has information because you can have a situation where someone is not able to consent just because they haven't been given enough information. It's a presumption of incapacity*

which a child has to overthrow, whereas with adults we presume capacity. We shouldn't put unrealistic obstacles in the way of children.'

Do local authorities give practitioners information/training in data protection and information security?

We asked local authorities to supply us with any information that they give to practitioners on data protection and on information security. We should say again that we are relying on their answers in order to assess provision and these may give only a partial picture.

Data Protection

The majority of local authorities replying to our request provide material to practitioners on data protection, but there is considerable variation in its range and quality. Four local authorities had clearly adopted the Information Commissioner's advice on supplying layered Fair Processing Notices. Twenty-two said that they provided data protection training sessions. Two said that they used films supplied by the Information Commissioner for practitioners and children. The remainder appear to provide written materials that range from specific data protection manuals to a brief mention of data protection included in other training material.

Eleven local authorities did not appear to be providing any information on data protection, although some of these may simply have chosen not to answer this section of our request. A further thirteen gave us some cause for concern because the content seemed minimal or focussed only on subject access requests. One or two said that information was 'made available' on the staff Intranet, but in our view this does not lay sufficient emphasis on the importance of data protection and relies on busy practitioners finding the information for themselves. We question whether this is adequate.

Information Security

Five local authorities said that they provide direct training in information security, and a further thirty-one have a security policy that is given to staff. Thirty-eight either told us that they did not have any information, or did not answer this part of our request. The remainder appear to supply limited advice to practitioners or make information available on the staff Intranet; two rely upon the broad undertaking that staff sign when they are given a password.

The security policies vary significantly in quality and content. A few give clear procedural instructions on every aspect of security, from choosing a password to the safe transmission of sensitive data. Typically these authorities mandate encryption for the transmission of all personal data and forbid the download of unencrypted information to portable devices. In one local authority, data can only be downloaded to encrypted devices with the consent of a manager and under the supervision of the IT department.

Other security policies are not so clear, containing injunctions to 'keep information secure', to 'choose an obscure password', or to 'share data securely', without actually explaining what this entails. Several make the rather ineffectual suggestion that, before downloading unencrypted information on to laptops or USB sticks, practitioners consider whether it is 'absolutely necessary'. In one or two cases we were concerned that the advice is simply not conducive to effective security. Two authorities instruct staff to lock confidential client files in the boot of their car if they are leaving it unattended. This is simply not safe, and we are concerned that a local authority could countenance having confidential data left unattended in a public place. Another authority asserts that it is safe to send sensitive data in a password-protected Word document via email to agencies outside the authority, but this offers little

protection when password-cracking software can be easily downloaded from the Internet at minimal cost.

We were surprised to find that only eight security policies mention encrypting sensitive data before transmission. A further two say that they expect to have encryption available soon; in the meantime practitioners are advised to password-protect documents. If security is to be effective, all local authorities should regard encryption as a standard feature and adopt rigorous security policies that are clearly communicated to staff. Dr Ian Brown, Senior Research Fellow at the Oxford Internet Institute points out:

> *'It is critical that systems are designed in a way that as far possible prevents security breaches, such as preventing sensitive data being copied onto unencrypted laptops, USB disks and other mobile media; and limiting very strongly the amount of sensitive data that can be copied around a system – eg it might be reasonable for a social worker to take home the records of 10 individuals on an encrypted laptop. It is a disaster waiting to happen for a director of children's services to take home information on hundreds or thousands of individuals, regardless of laptop encryption or any information security training they have received. This is in line with the Information Commissioner's recent report on "Privacy by Design".'* [27]

Until information security is treated as a priority in every local authority, it is difficult to see how practitioners can give any meaningful assurances to children about the security of their personal information. Indeed, poor security practices render consent itself meaningless if sensitive data can be lost, stolen or intercepted.

Conclusion and Recommendations

1. There is no basis in law for the Government's assertion in guidance issued to public bodies that a child in England can generally be presumed able to consent to the sharing of their personal and sensitive data from around the age of 12.

A child's age is not relevant to consideration of their competence to consent. Competence depends on the maturity of the child; the quality of the information provided to them; the nature and sensitivity of the data; and the child's understanding of the purpose(s) for which the data are shared, the organisations or individuals who will have access to their data and the consequences of consent, or of failure to provide it. It requires careful assessment of each individual child.

Many local authorities have adopted a presumption that a child is competent to consent from the age of 12, and some appear to be treating 12 as a *de facto* or *de iure* age of consent to data-sharing. In some cases this misunderstanding of the law has arisen from ambiguously-worded guidance issued by the Information Commissioner.

We recommend that Government guidance is amended to remove all reference to the age of 12; and that the Information Commissioner reviews the wording of his guidance to s66 of the Data Protection Act 1998 to ensure that it accurately reflects the law in England, Wales and Northern Ireland.

2. Few local authorities are providing training to practitioners in how to assess a child's competence to consent to the sharing of their personal and sensitive data.

We recommend that all local authorities are required to train practitioners in the assessment of children's capacity and competence to understand the reason for and the implications of sharing their data with specified organisations or individuals; and that they regularly review situations in which a child under 16 has given consent without parental involvement in order to ensure that correct procedures are being followed.

3. Parents have responsibility for their children. As a matter of good practice, parents should therefore be involved in the consent decisions of their competent children unless the child specifically objects, or there are special reasons against it. Several specialist lawyers whom we consulted believe this is a legal requirement.

We recommend that local authorities establish a default position of involving parents in decisions about any sharing of their children's sensitive data unless a competent child refuses such involvement. For non-competent children, the parents' consent should be sought and the views of the child taken fully into account; for competent children, the parents should at least be informed and consulted over such decisions unless there are obvious reasons not to do so, such as in cases of suspected child abuse.

4. In the context of the sharing of data on a child, information is also almost inevitably collected and shared about the child's parents and siblings. Some of this information can be highly sensitive or subjective. The law already requires that in such situations the parents should be made aware of this, subject to limited exceptions.

We recommend that this basic rule is followed in all cases, unless there are overriding reasons not to inform the parent, such as child protection concerns.

5. Children need clear information about the relative benefits and risks of data-sharing if their consent decisions are to be informed. Practitioners should have sufficient knowledge of data protection to enable them to give children this information in terms and in a manner that enables the child to fully understand it.

   The quality of information that local authorities give to practitioners about data protection and about language to be used with children varies significantly around the country. In some cases it appears to be inadequate or non-existent.

We recommend that the Information Commissioner produces a code of practice for local authorities, setting out standards for the provision of data protection training to practitioners, paying special attention to the protection of children's data.

6. Few local authorities appear to offer practitioners direct training in information security. The standard of the written information – if any – given to practitioners varies widely, and the inaccuracy of some security advice gives cause for concern. Few local authorities appear to have the ability to encrypt sensitive data downloaded to portable devices or transmitted to others via insecure networks.

We recommend that all local authorities are required to make encryption mandatory for the download and transmission of sensitive data; that the download of sensitive data on to portable devices is strictly controlled and supervised; that the Information Commissioner produces a code of practice setting out the minimum security standards to which local authorities should adhere; and that local authorities ensure that all staff are trained in the correct use of security procedures.

The Law in other European Countries

A brief comparative overview
Professor Douwe Korff

About the author:

Douwe Korff is a Dutch comparative and international lawyer and human rights- and data protection specialist. He is full Professor of International Law at London Metropolitan University and a member of the Advisory Council of FIPR (the Foundation for Information Policy Research). He has carried out four major data protection studies for the European Commission as sole author and is the lead lawyer in several further current EU-funded research projects. He was part of the FIPR team that produced the 2006 report, 'Children's Databases – safety and privacy'.

Acknowledgments:

I am grateful to the following people for having provided me with information and insights into their domestic law:

Belgium:
Prof. Yves Poullet of the Universities of Namur (FUNDP) and Liège (ULG) and Head of the 'Centre de Recherche Informatique et Droit'(CRID) in Namur, by email and in various conversations in the context of a project on which we both work.

Denmark:
Prof. Peter Blume of the University of Copenhagen and Mr. Jakob Lundsager of the Danish data protection authority (the *Datatilsynet*), in an interview held at the University of Copenhagen on 11 November 2008.

France:
Ms Marie George and Ms. Leslie Basse of the French Data Protection Authority (the *Commission Nationale pour l'Informatique et les Libertés* or *CNIL*), in the context of an earlier, wider study, carried out in 2006.

Germany:
Mr. Thorsten Koop of the Independent Centre for Privacy Protection of the German State of Schleswig-Holstein (*Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein* or ULD), which is the Data Protection Authority for that Land, in an interview held in Kiel, Schleswig-Holstein, on 3 June 2008.

Portugal:
Mr. Eduardo Campos of the Portugese National Data Protection Commission (the *Comissão Nacional de Protecção de Dados* or *CNPD*), in an interview held in Lisbon, Portugal, on 16 May 2008.

Spain:
Mr. Emilio Aced Felez of the Data Protection Authority of the City of Madrid (the *Agencia de Protección de Datos de la Comunidad de Madrid* or *APDCM*), by email and in various conversations in the context of a project on which we both work. I have also drawn on an article on Minors and new forms of consent by Ms. Ana Bayó, an Attorney with Clifford Chance in Barcelona, in Data Protection Law & Policy, Volume 5, Issue 6 (June 2008).

Sweden:
Ms. Katja Isberg Amnäs and Ms. Birgitta Åbjörnsson, of the Swedish Data Protection Authority (the *Datainspektionen*), in an interview held at the Authority's offices in Stockholm, on 12 November 2008.

Introduction

This paper is produced as part of a study of the law relating to the use of children's informed consent to the collection, storage and sharing of sensitive personal data on them. The study is carried out by Action on Rights for Children (ARCH) and funded by the Nuffield Foundation. The background is the widespread sharing of often highly sensitive personal data on children in the UK, in particular in the new context of the 'Every Child Matters' agenda. The data sharing, and the improper use of children's consent for this, was criticised by the Foundation for Information Policy Research (FIPR) in a study carried out in 2006, *'Children's Databases – safety and privacy'*.[28] The study also concluded that the data sharing was in violation of European law.

For the present study, ARCH is looking in detail at the law in the UK. This paper provides an additional, comparative-legal overview of relevant data protection law and practice in a number of other European countries: Belgium, Denmark, France, Germany, Portugal, Spain and Sweden. The information for most countries was obtained in the course of visits to those countries by the author. The information on France is based on earlier work, for the Children's Databases study mentioned earlier, and the information on Spain was obtained from a member of the Madrid Data Protection Authority in meetings in connection with that work, and through email. The information on Belgium is limited to one opinion of the Belgian Data Protection Authority to which the author's attention was drawn by a Belgian academic colleague just as this paper was being finalised. It is included in spite of the fact that no wider research into Belgian law had been conducted, because it is particularly interesting, both because of its own content and because of its reference to the law in other countries.[29]

The next section contains brief summaries on each of these countries, often based on somewhat larger papers on the country, submitted to ARCH in the course of the research. Some specific cases are included for illustration, but these are rare.

In section 3, the information is compared and analysed, with reference also to the UN Convention on the Rights of the Child (CRC)[30] and the EU 'Article 29 Working Party' Working Document on personal data on children.[31] That section also sets out some general conclusions on the comparative and European standards in this regard, and contrast them against the UK ones.

Law and practice in Continental-European countries

This section summarises the information on consent and data sharing with regard to minors in

the countries mentioned above. It starts with summaries of the situation in Germany and France, because the issue (and broader issues touching on it) have been addressed there in more detail than elsewhere. Next come Belgium, Portugal and Spain. Law and practice in Denmark and Sweden are summarised last.

Germany[31]

The German rules are important, because data protection is highly developed there, and the rules and principles enunciated by the German courts, and especially the Constitutional Court, have considerable influence also outside the country, in other European countries, and not least on the case-law of the European Court of Human Rights and the European Court of Justice.

It should be noted first of all, that in Germany consent as a basis for processing of personal data, especially by public authorities, is of limited relevance. More important are the requirements that any processing by such authorities may only take place for a narrowly-defined purpose and on the basis of a specific, strictly-worded legal provision, and that they may only seek and use personal data that are strictly necessary for those narrowly-defined purposes (as reflected in such strictly-worded provisions).[32]

Public authorities may not by-pass these fundamental principles by seeking the consent of data subjects for processing that is not already legitimate on these bases. Basically, therefore, they can only process personal data on the basis of consent to the extent that that is expressly allowed in the relevant rules, or clearly compatible with them.

Private bodies can in principle rely more broadly on consent – but subject to important restraints (which also apply to processing by public-sector bodies on that basis, where allowed). Any consent for any processing must be clearly free and specific, i.e. (to quote the Constitutional Court) for 'concrete, clearly-defined purposes' (*konkrete, klar-definierte Zwecke*). No-one, adult or minor, can give valid consent for ill-defined, unrestricted use of their personal data. In assessing whether a person was in a position in which s/he could give his or her free and informed consent, all the circumstances have to be taken into account: the *relationship* between the data subject and the body seeking the data; the *nature of the data; the uses (and disclosures) for which consent is sought and their proximity or otherwise* to the relationship between the data subject and the body seeking the data; the *importance and possible effects of the processing* for which consent is sought for the data subject; – and of course, last but far from least, the *capacity of the data subject* to appreciate the import of his or her consent (taking into account the *complexity* or otherwise of the matter at hand).

It is furthermore recognised that children are 'persons-in-the-making' and have a 'right to become [i.e., to freely develop into] a [full] person'. This means that they deserve *extra* protection, also in respect of their personal data, and that the general data protection rules and principles (such as the ones just mentioned) must be applied with *special rigour* when it comes to children and young people. The kind of sweeping, all-purpose 'consent' for data disclosures, also of highly sensitive information, in circumstances which may seriously affect the child or minor in question, as often relied on in the UK, would therefore undoubtedly be regarded as fundamentally flawed and invalid in Germany.

In the public and semi-public sectors, there are still further constraints. Even if an official or professional can process data on the basis of consent (which he or she often cannot, as just noted),

such consent will often be far from sufficient or conclusive – because such people are subject to broader duties that must be taken into consideration.

Specifically, for children between the ages of 12 and 14, the person dealing with the youngster – typically, a professional such as a doctor or teacher or social worker – must balance the different interests. For instance, a 13-year old can say that he or she wants to relieve a doctor from his duty of confidentiality, and let the doctor pass on medical data to a third person or party (say, an employer). The doctor *may* do this, but never simply on the basis of this request – not even if s/he feels that the child is mature enough to realise the implications. Rather, the professional must still always also exercise his or her professional duty or insight. Doctors and other professionals such as doctors, teachers or social workers first and foremost have a duty of care (*Fürsorgepflicht*) towards their patients, pupils or clients. If they feel, in their professional judgement, that it is better to first consult the parents, or indeed to refuse to act as requested by the minor, they are entitled to do so; indeed, failure to do so could be in breach of this duty. This duty, moreover, also extends to minors aged 15 or 16, or even 17.

In other words, there is no hard line (other than the absolute line, for all people without a mental deficiency, of 18). In respect of any young person under the age of 18, while the general rule is that they should in principle be seen as competent from the age of 14, the more important consideration is the professional duty of care. Accordingly, in the (quasi-) public sector, for children under 12, the parents should always be consulted; for children between 12 and 14, this must always be considered; and for minors over 14, it can still be considered from a professional point of view that it is necessary to consult the parents and not rely solely on the wishes of the data subject. This is the case especially if the professional feels that the minor is not in the best position to judge whether the request is in his or her best interest.

France[34]

France was one of the first countries in Europe – indeed in the world – to adopt a national data protection law, the Law on Informatics, Files and Freedoms of 1978.[35] The Law was substantially amended in 2004 to bring it into line with the EC Framework directive on data protection,[36] but the basic principles underpinning the Law, the basic regulatory approach, and the basic approach of the French data protection authority, the National Commission for Informatics and Freedoms or CNIL,[37] have remained the same.

For the present study, four matters are worthy of note. First of all, there is the general question of when a child can be said to be sufficiently mature to take its own decisions. In this respect, in France as elsewhere, the law accepts 18 as the overall age of majority, but nevertheless also gives certain rights to children of lower ages: At 12, a child can obtain a bank (ATM) card (with the consent of its parents); at 13, s/he must consent to a name change or to his or her adoption, and must be heard by a judge in divorce cases; at 15 girls may marry with the consent of at least one parent (for boys, the age is 18, except for special cases); 15 is also the age at which young persons can engage in sexual activity without criminal responsibility, and from which girls can obtain the 'morning after pill' and obtain an abortion without the involvement of their parents (if they don't want such involvement), provided they involve another adult; at 16, they can enter into a contract of employment (provided the parents don't object) and can join a trade union, apply for French nationality, and make a will (for up to half of their possessions). Children under the age of 13 are not criminally liable; children between 13 and 16 may only be held in pre-trial detention in exceptional cases of serious crime (*crimes*). There are also special rules on film categories and

on marketing to children of different ages. All in all, these various rules show that the legislator accepts that there is no one single cut-off point, but rather, that different criteria should be applied in different contexts.

Secondly, as concerns data protection, the French are weary of reliance on 'self-determination' and consent, and tend to take a more administrative-regulatory approach than the Germans, in that they seek to lay down (at least for the public and semi-public sectors) detailed rules setting out the data protection requirements for each specific context. The CNIL plays a central role in this, not just in monitoring compliance with data protection rules and principles laid down by the legislator, but by playing a strong role in the formulation of those rules themselves. It has a strong reputation as a forceful regulator, and also does not hesitate to play a dominant part in political discussions relating to matters within its competence. It takes a strong stand on questions of data protection law and minors, and stresses that *'the guarantees provided to anyone by [the French data protection law] must be applied with special force as concerns minors'.*[38]

A third matter of importance to the present study is the strong emphasis given, in France, to the duty to maintain 'professional secrecy' (*le secret professionel*). If anything, the legal duty not to disclose information held in a professional capacity is more strongly emphasised in law than are data protection principles against disclosures of personal information.

Fourth, as concerns minors of school age, it is important to note the basic principle that 'education overrides repression', i.e. that the best (educational) interests of the child should always be the primary concern, and that other public interests (such as prevention or detection of crime) are subsidiary to this when matters relating to an individual child are concerned.

Between them, the latter two principles – professional secrecy and the primacy of the interests of the child – tend to strongly emphasise the need for professional discretion: only the professional dealing with a child can decide whether confidentiality can be set aside in an individual case.

In various contexts, the CNIL has also strongly emphasised the need to involve parents in data protection matters relating to young people. Already in 1983, the CNIL ruled that questionnaires should not be handed out to (under-18) students in a secondary school (*collège*) without the prior written consent of the parents. In 1985, it adopted a general recommendation on the collection of personal information in schools (*en milieu scolaire*), which repeated this requirement and added further guarantees in respect of the use of psychological tests in schools. Since then, the CNIL has required the prior written consent of parents for the dissemination of photographs of minors on the Internet (e.g. on a school website) and for the passing on of contact data on minors for the purposes of direct marketing.

In a 2001 report on the Internet and the collection of personal data from minors (but which also touched on wider issues),[39] the CNIL expressly, and approvingly, quoted the preamble of the UN Convention on the Rights of the Child, which stresses that:

> The family, as the fundamental group of society and the natural environment for the growth and well-being of all its members and particularly children, should be afforded the necessary protection and assistance so that it can fully assume its responsibilities within the community.

Because of this, and because of the general need to protect children and parents, the CNIL held that all collecting of data from minors on their family circumstances, their parents' lifestyle and their social and professional status is 'excessive and unfair', and thus unlawful; and that the recording of

sensitive data on minors is also prohibited, unless the controller can provide proof that the parents have expressly consented to this.[40]

While set out in the particular context of the Internet, and more specifically to data collecting by private-sector bodies over the Internet, these principles should also be borne in mind in relation to the collecting of data on children in other contexts. Put simply, while there may be special justification for the collecting of data on children in the public sector, this too should be subject to strict purpose-specification and limitation; parents should be fully informed and in principle asked for their (written) consent; data on siblings and parents should not be obtained from children;[41] and the collecting and further use (and of course especially the disclosure) of sensitive data on children should be particularly strictly circumscribed, in rules drawn up by, or drafted following the advice of, the CNIL.

The general principles adduced above have so far been applied in only a few specific contexts other than the Internet; most did not deal with the question of consent.[42] However, the CNIL did touch on the issue in relation to the offering of services allowing people to check the place where a particular mobile telephone handset might be. The service is aimed in particular at parents wanting to keep track of the whereabouts of their children.[43] After holding an Internet poll on the issue, the CNIL merely posed the questions this service raised: Is it, the Commission asked, in the best (higher) interest of the child that its parents can determine where it is at any given moment? Indeed, is that legitimate?[44] In an earlier case, the Commission had held that 'web-casting' pictures from a crèche on a webpage intruded too much into the private life of the (very) young children in question. If that was so for a young child in a crèche, was it not also the case for a child or adolescent old enough to use a mobile phone?

More specifically, the Commission wondered if the use of such a service didn't, *'upset the normal interplay of trust between parents and children'*:

> *Doesn't this service, in a perverse way, tend to favour a disengagement of parents who may get the illusion of being in charge of – or at any of being able to check – the activity of their children?*

And finally:

> *From a societal point of view, doesn't the development of such services tend to get individuals used, from an early age, to a form of semi-permanent surveillance, so that he is not even any longer aware of the intrusiveness of such measures?*

It is clear from these and other comments and somewhat rhetorical questions that the CNIL has great doubts about the 'legitimacy' of the service. More generally, and more directly relevant to the present study, it is clear that the Commission lays great score by the need to allow young people their own space, and is fearful of a society in which technology is used to ever-increase surveillance over the actions of youngsters and adults alike.

However, that does not mean that parents should not normally be involved in matters touching on the privacy of their children. Thus, the CNIL authorised the use of hand contour technology in a number of schools, to control access to the canteen by pupils, because (the CNIL believed) the technology did not leave traces on the use, by individual pupils, of the facility.[45] However, even for the schools authorised to use the technology, the CNIL ordered that the legal guardians of the pupils should be individually informed of the new system, and that they should be given the opportunity to refuse to allow the use of biometric data on their children – even for the approved (non-trace-

leaving) systems. The schools should therefore provide for an alternative means of allowing access to the canteen for those children whose parents objected to the hand-contour access system.

The sharing between public bodies of personal (and indeed sensitive) data on minors would, in France, first of all require a clear, specific legal basis, which should spell out the precise purposes and limitations of the data sharing. The CNIL would be highly doubtful of the legitimacy of basing any such sharing on consent, and would be likely to find (similar to the German data protection authorities) that consent could not be relied upon in the absence of such provisions. Where, exceptionally, it might allow it (or where the law might expressly envisage it), it would appear that the CNIL would require such consent to be given by the minor's parents, at least as far as younger minors (say, under the age of 15 or 16) are concerned.

Belgium

The issue of consent by minors to the processing of their personal data has been addressed in some detail in Belgium in an Advice by the Belgian data protection authority (the *Commissie voor de Bescherming van de persoonlijke levenssfeer/Commission de la protection de la vie privée*, or Privacy Commission) in relation to the protection of the privacy of minors on the Internet.[46] Apart from dealing with the specific issue of children and the Internet, the Advice also summarises when a child, in law, reaches maturity, and sets out some more general principles and considerations with regard to the processing of personal data on children.[47]

On the question of when a child comes of age, the Advice notes that although under Belgian law, the general age of maturity is 18, in reality – and law – there is a gradual development, with minors gaining more independence as they grow up, in particular in adolescence (put at broadly 13 – 16). Thus, the rules on television content give special protection to children under 12; and the rules on toys, to children under 14. A child can have a bank account, and draw on it, from the age of 16, and that is also when s/he can go to see certain cinema films, drink alcoholic beverages, and ride a moped. Youngsters over 16 are also given standing in certain legal proceedings under the Civil Code, and can independently enter into many contracts (but not all, with there being restrictions, e.g., in the context of employment contracts).

The Privacy Commission deduces from these rules the general principle that minors in general, and especially children who have not yet reached a certain maturity, must be given special, additional protection in data protection law. The Advice is not very clear on when children can be assumed to have reached such maturity, apart from stressing that this will depend on the practical and legal context, and will usually lie somewhere between the ages of 12 and 14. But in contexts such as those considered for the present study, i.e. the collecting of often highly sensitive data on minors, for the purpose of sharing those data between various bodies, long-term and for a variety of possible purposes, it may be assumed that the threshold should be set high: at least 14, if not 16. Hereafter, I will refer to children under this age as 'young minors'.

This translates into a number of specific requirements, again formulated with specific reference to the Internet, but in terms and subject to explanations that clearly can be more broadly applied.

Thus, the Advice notes that when s/he is in touch with others over the Internet, a child is in a weak position, because s/he is more easy to manipulate, less suspicious, and less aware of rights than adults – but those matters of course also apply outside of 'Cyberspace'. It adds that while the Belgian Data Protection Law does not contain any special provisions on children, it does contain

many provisions that are couched in flexible terms and allow for judgment and discretion in their application, and require a balancing of the interests of the parties concerned (in particular, the data controller and the data subject). The Law must generally be applied, in many contexts, in a way that takes into account the existing imbalance between the controller and the data subject.

It follows that the following principles in particular must be applied strictly when it comes to children: the principle of transparency in the information provided to the data subject (the child); the principle that all processing of personal data must be lawful and based on a criterion that legitimises the processing; and the principle that there should be strict limits on the data that are being collected (and, one might add, on the use and in particular any secondary use or disclosure of those data).

The Advice expands on each of these principles, as applied to children, more specifically in relation to their activities on the Internet. Without going into too much detail, these clarifications can be summarised as follows:[48]

As concerns the **informing** of data subjects of the usual details (identity of the controller, purposes of the processing, etc.), the Advice stresses the need to adapt the language to the age of the data subject: the text must be simple and accessible, and the controller must use a direct style personally addressed to the minor. The controller must explain why the data are sought and are necessary, and that the data subject/minor will retain control over the data. The Advice adds that:

> *The minor must be encouraged to inform his parents of his on-line activities, let them take part in them and ask them for their views before transmitting his or her personal data.*

And a little later, as concerns **purpose-limitation** and **data disclosures**:

> *Data that were collected [from a minor] in a specific [on-line] context, may in no case be used for other purposes than those for which they were collected and of which the data subject was informed in the course of the data collection.*
>
> *In order to protect minors, they should moreover not be passed on to others.*

In other words, contrary to general data protection law, data on children may not be used for purposes that are 'compatible' (or to be precise, 'not incompatible') with the original, stated purpose(s), and may not be passed on to third parties even where data on adults might, in similar circumstances, be so passed on. Of course, those remarks are specific to the context of children's activities on the Internet. But they do show the very strict approach to the application of the Law to children generally.

The Advice is also very strict on other points, and in principle regards as **illegitimate and unlawful**: the collection of data from young minors for direct marketing purposes; the collection of data from young minors on their personal environment, such as their parents or siblings, or their fields of interest ('lifestyle data'); and the collection of data from them through games or offers of gifts. The Privacy Commission goes on to address the question of obtaining **sensitive data on children**:

> *Under the Law, in principle no sensitive data may be collected at all from [young minors]. In some special cases, in which the passing on of health data of the minor must be done over the Internet, the processing should only take place with parental consent, on condition that the other requirements of the Law (in particular, the provision of detailed information by the controller about the conditions for the processing) are complied with.*

The Advice similarly stipulates that for the dissemination of photographs of young children, the express and specific consent of the parents is required, and that this consent cannot be obtained in a more general form, also covering other matters: there must be a form, to be signed by the parents, which specifically details the matter and, e.g., allows parents to give permission for the publication of class photos on a school's website, without agreeing to the publication of individual photographs.

There is indeed a complete section on parental consent in relation to processing of personal data on children. Although of course drafted in the particular context of children's activities on the Internet, this section has wider application, and may therefore be quoted in full:

> ***Concerning parental consent***
> *The [Privacy] Commission feels that parental consent is not systematically required every time personal data on children are processed on the Internet. It wishes to underline that parental consent should not be turned into a mechanism that works against the best interests of the child, unless there is a serious risk that the child cannot correctly assess the real implications of its decision, or when its naivety is exploited.*[49]
>
> *The Commission therefore emphasises in this document the need to obtain parental consent in specific circumstances, i.e.:*
>
> - *when the child has not yet reached the age of maturity,*
> - *when sensitive data are collected,*
> - *when the purpose to be achieved is not in the direct interest of the minor (marketing, disclosure of the data to others),*
> - *when the data are intended for publication ([e.g.,] dissemination of information through a discussion forum, or on the website of a school).*

It is important to stress that these are all alternative situations in which parental consent is required, i.e., such consent is required: in *all* circumstances when the child is not yet mature enough to understand the implications of the solicited consent (which is generally 13 – 14, but for complex cases may be 14 – 15); and in *all* circumstances in which sensitive data are sought from a minor, even an older, 'mature' minor (under 16); and in *all* circumstances when the processing may not be in the *direct* interest of the child (or, one might add, when there may be doubts in that regard, and/or when the parents might reasonably have a different opinion on the matter than the body seeking the consent).

These considerations are clearly relevant also to the kinds of issues examined in the present, wider study.

Portugal

Although Portugal has had a data protection law since 1998 (based, like the other laws in the EU, on the EC Directive on data protection),[50] the standards under this law have not yet been fully developed,[51] and there is little specific law on its application to minors, although the issue has been raised in one specific context: as concerns children in care. However, that one issue has unfortunately been taken out of the hands of the Portugese National Data Protection Commission (CNPD).[52]

In Portugal, as in many other, rather conservative South-European countries, the 'old' view was that until the age of maturity (traditionally often 21, or even older, but now usually 18), minors were '*in manu*': they were under the guardianship of their parents. And then, suddenly, at 21 (or 18), they became full persons in the eyes of the law, with very little transition between the two periods. This view has developed, however, and nowadays the situation is more nuanced – also in law. There are two or three broad demarcation lines.

First of all, until 12, a child is still basically regarded as being under the tutelage of the parents, without any right to assert its own rights (except for very special cases). Between the ages of 12 and 16 (now 14: see below), a child's opinion is important but not decisive: the child must be heard, e.g., in family cases, but that is all. From the age of 16 (now 14), the child's opinion must be given very serious consideration, and will often be followed, although it is still not decisive. As already indicated in brackets, very recently, this latter threshold has been lowered from 16 to 14. And of course, from 18, the young person becomes fully legally competent. So basically, the law gives increasing weight to the view of a minor, depending on the minor's age and individual maturity, and taking into account the nature and seriousness of the matter in question.

However, there is also a second principle at play: that the interest of the child is always paramount. Everyone who deals with a child, a minor, must always act in the child's best interest. This applies to teachers, doctors, social workers, police officers, the courts – everyone. Crucially, it is accepted that the best interest of the child will often demand that the child's parents are consulted on a decision affecting the child, if only because the parents can thereby help to ensure that all relevant considerations are raised.

In addition, there may be further considerations of a general constitutional/administrative law kind, similar to the ones that apply in Germany, as discussed above, that limit the rights of public authorities to act on the basis of a citizen's consent generally in the absence of more specific statutory authorisation. However, such general principles have not been developed in Portugal as strongly or clearly as in Germany.

How these basic principles and considerations should be applied in a data protection context has not yet been formally clarified. However, the basic approach is clear. Processing of personal data on a child under 12 cannot be based on the child's own consent: instead, the child's parents' consent should be obtained. A child between the ages of 12 and 14 may be able to exercise some data protection rights in its own name, perhaps even without involving the parents at all, if the matter is relatively trivial – say, a child seeking access to its own library records. But if the issue is serious and may affect the interests of the child, its parents should be informed and consulted, and are likely to be given an overriding right to decide. If the child is over 14, its views will be given more weight, and may be decisive, but the data protection authority is still likely to feel that, in the absence of special considerations against this, the young person's consent cannot be considered valid if the parents have not at the very least been consulted. And overall, the data protection authority will still, for all minors, place a great emphasis on the need to consider what is in the minor's best interest.

The latter would mean that no-one, and in particular no professional, official or public organisation, can simply rely on the consent of a minor to legitimise processing of personal data (and *a fortiori* sensitive personal data) on a minor. As just noted, in all but the rarest cases (typically, concerning suspected child abuse by parents) parents must be consulted.

In addition, in all cases, the interest of the child must be considered, and given pre-eminence.

Crucially, in the end, the Portugese data protection authority will feel competent to make this assessment, and if needs be to override the parents' views.[53]

Spain

In Spain, the main EC Directive on data protection was implemented by means of a new Data Protection Law, adopted in 1999 by means of a Regulation, which replaced the previous Law of 1992.[54] However, the new Law (or, to be more precise, the Regulation implementing the new Law) was only approved, and thus brought fully into force, by means of a Royal Decree issued in December 2007.[55] The Regulation provided some amendments and additions to the 1999 Law, and one of these specifically concerns consent for the processing of personal data on minors. It came into force on 19 April 2008.

Broadly speaking, in the public and quasi-public sectors, processing of non-sensitive personal data must either be based on the consent of the data subject, or necessary for 'the exercise of the functions proper to public administrations within the scope of their responsibilities' or for the maintaining or fulfilment of an 'administrative relationship' (Article 6(1) of the Law). However, for the processing of sensitive data in those sectors, explicit consent or specific authorisation by law is required (see Article 7(3) of the Law in particular; cf. also Article 12(1), first sub-clause, of the Decree).[56]

Article 3(h) of the Law and Article 5(1)(d) of the Regulation define the data subject's consent generally, in accordance with Article 2(g) of the Directive, as:

> *any free, unequivocal, specific and informed indication of his wishes by which the data subject consents to the processing of personal data relating to him.*

Paragraphs (1), second sub-clause, and (2) of the Regulation add to the general requirements for valid consent *inter alia* the following elaborations of interest to the present study:

> *1. The request for consent shall refer to specific processing or series of processes, stating the purpose for which they are collected, as well as the other conditions applying to the processing or series of processes.*
>
> *2. When consent of the data subject is requested for the assignment [read: disclosure/sharing] of his data, he shall be informed in such a way as to understand unequivocally the purpose for which the relevant data shall be used and the type of activity performed by the recipient. Otherwise, consent shall be null and void.*

Most important for the present purpose is the fact that – unique in the EU – the Regulation adds to this a specific provision on the question of consent for the processing of data on minors. The provision, contained in Article 13 of the Regulation, reads as follows:

Article 13 – Consent for the processing of data on minors

> *1. Data pertaining to data subjects over fourteen years of age may be processed with their consent, except in those cases where the law requires the assistance of parents or guardians in the provision of such data. The consent of parents or guardians shall be required for children under fourteen years old.*

> *2. Under no circumstances may data be collected from the minor regarding information about any other member of the family unit, or about its characteristics, such as data relating to the professional activity of the parents, financial information, sociological or any other such data, without the consent of the persons to whom such data refer. The aforesaid notwithstanding, data regarding the identity and address of the father, mother or guardian may be collected for the sole purpose of obtaining the authorisation set out in the previous subsection.*
>
> *3. When processing refers to the data of minors, the information aimed at them shall be expressed in easily understandable language, with express indication of the provisions of this Article.*
>
> *4. The data controller is responsible for setting up the procedures that guarantee that the age of the minor and authenticity of the consent given by the parents, guardians or legal representatives have been effectively checked.*

This provision is of interest in several respects. First of all, and in a comparative-legal context somewhat unusual, is the stipulation of a specific age limit – 14 – under which consent for processing of data on a minor must be obtained, not from the minor but from his parents or guardians, and above which the minor's own consent can in principle suffice. However, the latter (note: not the former) is subject to the qualification '*except in those cases where the law requires the assistance of parents or guardians in the provision of such data*'. I understand that such requirements are often contained precisely in the kinds of contexts examined for the present study: education, the provision of social welfare, health, etc.

Also notable is the strict prohibition ('under no circumstance'/'*En ningún caso*') on the collection, from a minor, of any information about his or her parents or siblings (or indeed others belonging to the 'family unit' (*grupo familiar*), such as grandparents or others living with the family), or about their financial or social circumstances: such data may only be collected from those other family members themselves. This means that, in practice, the collecting of data on minors directly from them will be very limited, and cannot begin to get close to the amount and nature of data that are collected on minors (and their families) in the UK.

If sensitive data were to be collected from minors over the age of 14, on the basis of their supposed consent, it should furthermore be noted that the authorities (in particular, of course, the different Spanish data protection authorities)[57] would be extremely strict in applying the rules on the validity of such consent, mentioned above.

Denmark

In Denmark, young people generally become legally competent at the age of 15, but there are differences in different context. Rights and duties may start at different (lower or higher) ages for social security (welfare) benefits, in the context of civil procedure, etc. Of interest to the study is the fact that in the context of requests for abortion by young girls under the age of 15, normally the parents should be involved, but if there is a problem with that, a special committee can decide. Another general matter of interest to this study concerns the use of the national identity number. This is widely used in the public sector for data sharing. But it is subject to a rule that the data subject must be informed of the fact that his or her data are being shared.

There are no specific rules in the Data Protection Law on its application to minors. The general rule

about youngsters from the age of 15 being legally competent is usually taken as a rule of thumb also in the data protection context – and thus also in a data sharing/use of the ID number context. In that latter context, it would therefore generally be the parents who are informed of the sharing of data on their children under the age of 15, but young persons over that age would normally themselves be informed (rather than their parents). However, the authorities stress that this is only a rule of thumb: in any particular case, all relevant matters should be taken into consideration, including the nature of the data, the seriousness of the issue in the context of which the data are processed or shared, and where appropriate the maturity or otherwise of the young data subject. All of these may imply a need to involve the parents, and to not solely rely on the consent of the young person, even if s/he is over the age of 15.

Example: There has been one special case relating to children in Denmark. This concerned an Internet chat room, organised by the organisation *Børns Vilkår* (Childrens' Rights), through which children can 'talk' in private, seemingly anonymously, to an adviser (but with their IP address recorded).[58] The data protection authority held that the record of the IP address sufficed to bring the issue within the data protection law, which meant that consent was required for the processing of the (sensitive) personal data on the callers. The authority stressed the strict general requirements of the law as concerns consent generally: it has to be free, specific and informed, it must relate to a specific (concrete) matter, and it must be explicit although not necessarily in writing; on the Internet, it can be given by means of a 'click' on a 'yes' (or 'I agree') button.

The authority held that *in this particular case* it could accept that the children that contacted *Børns Vilkår* could give the required consent, taking all the circumstances into account. But it emphatically underlined that this was a one-off decision, applicable to this particular case and this particular website, run by this particular organisation, only. It expressly reserved the right to examine any other, even similar cases, on their own merit.

(Vedrørende rådgivning i chatrum [concerning counselling in a chatroom], advice from the Danish data protection authority, the Datatilsynet, of 2 January 2002)

Sweden

In Sweden, the basic rule is that children of 14, 15, perhaps 13, are normally capable of giving consent for the processing of their data – but this is always subject to a test of whether the individual child in question is mature enough. Professionals may never simply rely on the age of the child; rather, they must always take the context and the maturity of the particular child into account. Moreover, even if a child is deemed to be capable of giving consent, the parents must still be informed of the fact that the child consented to any specific processing or data sharing (unless there are special reasons not to do so, as in cases of suspected child abuse).

If it is proposed to use data on children for research purposes, the research must be approved by an ethics committee, *and* the child must give his or her consent (if s/he is 13, 14 or 15 and mature enough), *and* the parents must also give their consent.

Further rules, giving more specific guidance, can be found less in the Data Protection Law than in other laws, such as laws on education, health, welfare, etc. Also relevant are the rules under the Secrecy Law, which are however implemented not by the Data Protection Authority but by a special

unit in the Ministry of Justice. The Ombudsman, too, can intervene in relevant cases and thus steer practice in this regard, although there are few if any known cases.

Finally, it may be noted that a review is taking place of data sharing arrangements, in particular in the public sector (not limited to children). The report on this review is due in the autumn of 2009.

Comparison, Analysis & Conclusions

The above shows that there is no easy, simple consensus between the Continental-European countries examined on the question of when a minor can give his or her consent to the processing of his or her personal data. There is in particular no agreement on a specific age when this can be said to be the case. On the contrary, the consensus is that this is not a matter that lends itself to such a simple rule. As further discussed below, that is even true for Spain, where a recent Regulation does stipulate a specific age – 14 – when, in principle, minors become competent under data protection law.

Rather, the issues and the answers to the issues are complex, and many other factors than just age should be taken into account (both generally and specifically in relation to children). Once that *caveat* is understood, there is quite considerable agreement on the principles and considerations concerned. Some more country-specific issues remain – but even on those, there is quite considerable convergence.

As often, the thinking on this is most developed in Germany and France. However, the law and approach in the other countries quite notably chime in with them, and add some further, useful detail.

Crucially, in most Continental-European countries there are preliminary issues to be taken into account before one can even begin to think about the specific question of consent by minors. Thus, in Germany, consent (even of adults) can only rarely be relied upon by public authorities as the basis for the processing of personal data: much more important is the question of whether there is a specific, tightly-worded legal provision that authorises the processing for clear, narrowly-defined ('concrete') purposes. Public bodies are simply not allowed to rely on the consent of anyone to collect and further process personal data without such a clear statutory authorisation. One can read similar (constitutional) restrictions into the law in other countries, including Spain and Portugal, even if they are not quite as developed. France, too, is extremely wary of processing on the basis of consent. Processing of personal data by public bodies in that country too may only take place on the basis of specific rules – and often, in addition, only after the data protection authority (the CNIL) has been given the opportunity to give its 'views' (Avis) on them – and those views are rarely ignored.

The data protection laws on the Continent are moreover generally strict about what constitutes valid 'free, specific and informed' consent – again, in any case, be this of an adult or a minor. In all the countries examined, valid consent can only be given by someone (adult or minor) if that person was fully aware of, and could appreciate, the consequences of giving his or her consent, which in itself means that consent can only ever relate to specific, clearly-defined processing for very specific purposes. One simply cannot give valid consent for general processing or sharing of one's personal data for ill-defined purposes, and/or when it is impossible to fully understand the implications of the consent. Nor can consent be valid if it is obtained under pressure, e.g., if one is told that unless one consents one will not receive a certain public service like health care, or welfare.

On the Continent, it is furthermore expressly recognised, not just by the data protection authorities but notably also by the courts (most specifically the German Constitutional Court, but also the highest Belgian, French, Spanish and other national courts), that minors are 'adults in the making', who require extra protection of their fundamental rights, and thus also extra data protection (which is usually a constitutionally-protected fundamental right in those countries). In other words, the above rules are, in all the Continental countries examined, applied with special rigour in the case of minors: statutory authorisation for the processing of personal data must be especially clear and precise, for especially clearly-defined purposes, and strictly necessary and proportionate to those purposes. Reliance by public bodies on the consent of minors to by-pass those legal rules is subject to especially close scrutiny and highly likely to be regarded as invalid (if it is not expressly banned altogether, or made subject to further conditions, as discussed below).

On children's consent, there is general agreement between the authorities in the different countries that in order to assess whether it is valid, all relevant circumstances must be taken into account, such as: the nature of the data, the context in which the data are collected, the importance of the processing and its possible effect on the minor, the capacity of the individual minor, and the complexity of the issues.

An opinion issued by the Belgian data protection authority on the collecting of personal data from minors over the Internet provides some clarification of the strict approach in that context: it says that the minor must be informed in especially clear language, adapted to their age; that the legitimate basis of the processing, such as consent, must be especially clearly ensured; and that the data are subject to an absolute limitation on use for the specified purpose only (i.e., they may not be used for 'compatible' purposes). The opinion also imposes strict limits on any data collected: it says it is illegal to collect any data from minors for the purpose of direct marketing, or any sensitive data, or any lifestyle data, or data on the family (parents and siblings), or more generally, whenever the data are collected for processing that is not in the direct interest of the child. For any such data collecting, parental consent is required. The child must in any case be encouraged to consult and involve their parents.

These limits are reflected more broadly in the laws and rules in other countries, also beyond data collecting on the Internet. The Regulation in Spain quite generally stresses the need for especially clear language to inform minors. The French data protection authority also holds the view that, especially (but not only) in relation to the Internet, parental consent is required for the collecting of sensitive data on minors, or of data on the parents and siblings and wider family situation of a minor. It has similarly demanded parental consent for the use of questionnaires in schools, the release of school photos on a school's website, and the use of hand contours in access to school canteens. In Germany, collection of data from a minor (or indeed, anyone) on other family members would breach the rule that all personal data must, in principle, be obtained from the data subjects: data on parents and siblings should be obtained from the parents or siblings themselves, and not from the child being questioned. In Sweden, parents must at least always be informed of any collection of data on their under-age children (with some special exceptions). The same applies in Portugal whenever significant interests of the child are involved, and that even applies to older minors. Most notably, in Spain, where the Regulation seems to provide for a specific age from which a minor is deemed data-protection competent, the law nevertheless adds that no lifestyle data or data on the family (parents and siblings) may be collected from such a 'competent' minor. This means that, in spite of this age-stipulation, in practice only the most trivial data can be legally collected from such a minor without the parents at least being aware of it. In Denmark, the involvement or otherwise of the parents is one of the circumstances that can be taken into account in determining whether a minor's consent was valid – which means that consent for processing that

may have significant implications for a minor may be considered invalid if the minor did not involve his or her parents.

This heavy emphasis on the involvement of parents is fully in accordance with the approach adopted in the UN Convention on the Rights of the Child, which stresses the importance of the family (as the French data protection authority expressly noted). Not only do parents have a right to be involved in decisions on, of and by their children. Children, too, have a right to involve their parents in the decisions they take – and should be encouraged to do so. That is not to say that children are not also entitled to their own 'space': on the contrary, as the CNIL also noted, some services, such as gadgets that allow parents to know at all times where their children are, or CCTV monitors in nurseries, accessible to the toddlers' parents, can be too intrusive. But those are separate matters.

It is only against this background that the question of the age of the child is considered, and even then, the issue is still subject to a further consideration, which will be discussed later. In that regard, (somewhat) different specific ages are mentioned in different countries, but with nevertheless again a quite remarkable convergence in application. Thus, as we have seen, the recent Regulation in Spain specifically sets the age at which minors are deemed to be competent in data protection matters at 14 (but hedges this about with safeguards). In Germany, too, the data protection authorities see 14 as an important age in respect to data protection matters (but without that being a fixed age). In France, children aged between 13 and 15 are seen as increasingly competent, but for matters that can have serious implications, the data protection authority would tend to look at the higher rather than the lower range. In Portugal, 14 has also become a crucial age: the views and wishes of children between 12 and 14 are important in various contexts, but not decisive, but those of minors over 14 are usually, or at least often, decisive (children under 12 are still fully *in manu*). Belgium takes a similar position, with the upper age perhaps somewhat higher, at 14 to 16. And in Denmark, young persons are quite generally deemed competent under the law from the age of 15 – but this is still subject to the requirement, noted above, that in deeming whether the supposed consent of such a young person is valid, all the circumstances must be taken into account, including the question of whether the parents were consulted.

The broad consensus therefore seems to be that the 'rule of thumb' is that in the Continental-European countries examined a young person will often be able to consent to processing of his or her data by him- or herself from the age of (roughly) 14, 15 or 16 – but with the precise question of whether a particular minor was competent and, more importantly, had given valid consent in a particular context still depending on all the circumstances, including both subjective matters such as the maturity of the minor and more objective matters such as whether the matter for which consent was given was in the direct interest of the minor or not, and indeed whether the parents were, or should have been involved. For trivial matters, or matters which do not have any significant effect, the age may be lower, sometimes perhaps as low as 12, but even then the requirements about the validity of consent (free, specific and informed) remain to be met, and are strictly applied. In Denmark, the Danish data protection authority stressed that a ruling that relatively young children were competent to seek advice from a (reliable) children's organisation's website was highly case-specific and should not be seen as undermining the general approach just mentioned.

There is one final, crucial matter. This is that in all the countries examined the entire framework described above is still subject to one additional, overriding test, which is whether the 'best interests of the child' are served by the processing for which consent is sought. This principle – which of course also underpins and permeates the UN Convention on the Rights of the Child, ties in with another fundamental matter: the duty of professionals dealing with minors to carry out their tasks in a highly professional manner, under a strong duty of care towards the minors, and subject to

professional rules that should stress confidentiality and respect, and the best interests of the child.

In Germany, a professional faced with a request by a minor to allow a particular use or disclosure of his or her data must consider whether this use or disclosure is in the minor's best interest, whether it is better to consult the minor's parents (subject to the professional's duty of confidentiality), or even whether to refuse to comply with the request – even if it is made truly and freely by a 'competent' minor. In France, professional secrecy and the principle that 'education overrides repression' also combine to strongly underline the duties of professionals to exercise professional discretion in such matters, and not to simply rely on requests from, or the consent given by, a minor. Similar duties are imposed on professionals – doctors, school nurses, teachers, social workers, etc. – in all the other Continental-European countries.

In these countries – which I believe are representative of all the Continental-European ones – the above creates a strict framework for the processing of personal data on minors, and their families (and of course especially for the processing of sensitive data, or of data which may significantly, or long-term, affect a minor or his or her family).

That framework is much stricter than the one in the UK. Briefly, in the Continental-European countries, public bodies may not rely on open-ended, vague *vires* clauses to ask children for information on themselves and their families for all manner of ill-defined processing and sharing, and they cannot simply try to obtain consent from a minor to process his or her data without a clear legal basis. In the Continental-European countries, the requirements for consent (free, specific and informed) will be very strictly applied to minors. The consent of no-one, but especially not minors, can be said to be 'free' if it was given under threat of loss of a service or help. Moreover, in the countries examined, the consent of even 14, 15 and 16-year olds will often not be valid unless the parents have been involved; it will suffice for 12 – 14-year olds in only the rarest cases. And in any case, even if a relatively mature and competent older minor asks for certain uses or disclosures of his or her data, and gives valid consent for it, any professional involved will still have to exercise his or her professional duty of care, and may demand parental input or refuse the request altogether.

Footnotes

1 Children's Privacy Protection Network: Terms of reference http://www.privacylaws.com/upload/cppntermsofreference.doc

2 Information Sharing: Guidance for practitioners and managers, p18 HM Government 2008

3 Woolf, J [1984] Q.B. 581, Court of Appeal [1985] 2 W.L.R. 413, House of Lords [1986] 1 AC 112

4 (1883) 24 Ch.D. 317

5 [1970] 1 Q.B. 357

6 [1991] 3 WLR 592

7 [1992] 3 WLR 758

8 [1999] 1 FLR 672

9 [2005] 1 FLR 236

10 [2004] 2 FLR 949

11 In relation to vulnerable adults, see *E (by the Official Solicitor) v. Channel Four, News International Ltd and St Helens Borough Council* [2005] 2 FLR 913

12 [1996] 2 WLR 88

13 [2006] 3 WLR 599

14 s1(1) Children Act 1989

15 [2006] EWHC 37 (Admin)

16 Bristol Children and Young People's Services: http://www.bristol-cyps.org.uk/schools/fair-processing-notice.html

17 Overarching Information Sharing Protocol, Children and Young People in Wolverhampton

18 HL Debates 01 July 1991 vol 530 cc866-82 http://hansard.millbanksystems.com/lords/1991/jul/01/age-of-legal-capacity-scotland-bill

19 Age of Legal Capacity (Scotland) Act 1991 (c. 50). Crown copyright.

20 'Transaction' is defined at s9 and includes 'the giving by a person of any consent having legal effect'

21 Data Protection Act 1998, CHAPTER 29. Crown copyright.

22 Data Protection Act 1998, Legal Guidance. http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf

23 s3 Children Act 1989 C.41 Crown copyright

24 Common Assessment Framework for children and young people: practitioners' guide, p.20, Children's Workforce Development Council 2007.

25 Information Sharing Guidance for Practitioners and Managers, HM Government 2008

26 *Mabon v. Mabon* [2005] EWCA Civ 634

27 *Privacy by Design*, Information Commissioner's Office, 2008

28 See: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_issues_paper_protecting_chidrens_personal_information.pdf.

29 Cf., however, the author's earlier general review of the Belgian Data Protection Law in his *Country Report on Belgium*, included as an appendix on a CD-ROM issued with his book on *Data Protection Law and Practice in the EU*, Brussels/New York, 2005.

30 Full text at: http://www.unhchr.ch/html/menu3/b/k2crc.htm.

31 Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools), WP147, adopted on 18 February 2008. The full text can be found at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm.

32 Note that the German rules described in this sub-section derive mostly from constitutional law and -principles, rather than from the specific Federal Data Protection Law, the *Bundesdatenschutzgesetz* (latest version of 2001, adopted to implement the main EC Directive on data protection, and which amended the 1990 version, which replaced a yet earlier [1977] Federal Data Protection Law in order to give effect to the seminal *Census*-judgment of the Constitutional Court, of 1983), although the Federal DP Law, and many more specific data protection rules on other laws, of course do also reflect those principles.

33 Cf. the general provisions in § 1(1) of the Social Welfare Law (*Sozialgesetzbuch* or SGB), which are similar to the British vires clauses but which in Germany are not sufficiently specific in themselves to serve as a basis for the processing of personal data, and the much more specific provisions in §§ 11 – 14, 16 – 20 and 22 -25, which do allow for it, quoted or paraphrased in the more detailed report on Germany, on pp. 5 – 6.

34 This sub-section largely consists of shortened excerpts from a report on the law in France on data protection as applied to minors, written by the same author for the 2006 FIPR/ICO study on Children's Databases (footnote 1, above) and contained in the report on that study as *Appendix B: The Legal and Regulatory Framework in France* (pp. 168 – 183). I understand there have been no major developments or changes in the situation in the country since then.

35 *Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

36 By means of the *Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004*.

37 *Commission Nationale de l'Informatique et des Libertés.*

38 *Internet et la collecte de données personnelles auprès des mineurs*, report prepared by Mme Cécile Alvergnat (member of the CNIL) and adopted on 12 June 2001, p. 31. See the text below for more on this report.

39 *Internet et la collecte de données personnelles auprès des mineurs* (footnote 11, above).

40 *Idem*, pp.31 – 32. The report adds that parental consent is also necessary for the passing on of data on minors in connection with the playing of games or the holding of lotteries etc. on the Internet.

41 While not as formally stipulated as in Germany, France too adheres to the principle that whenever possible personal data should be obtained directly from the data subject, rather than indirectly, from others, in that collection from others will often be regarded as 'unfair' and thus contrary to the Law.

42 See the Children's Databases report (footnote 1, above) for descriptions of these cases. Briefly, in 1981, in relation to the so-called GAMIN system, the CNIL ruled that children should not be identified by computer as likely to need medical or social assistance. That case did not relate to processing on the basis of consent (except that the decision implied that such 'profiling' would not even be allowed with the consent of the data subjects, be that a minor, or their parents, or both). And in 1986, the CNIL issued strict rules to be applied in the operating of a National Student Database, *Scolarité*, which greatly restricted the disclosure of data on individual students by schools and colleges to central authorities. In that context, it held that beyond the very limited disclosures allowed by those rules, no data should be passed on to third parties *'without the written consent of the student him/herself if s/he is legally competent, or his/her legal guardian, unless otherwise provided by law.'* (Art. 5 of 'simplified norm' No. 29 of 2 December 1986). However, it did not clarify the matter of when a student should, in this context, be considered legally competent (*en la capacité*). If anything, the wording implies that the ordinary general age of 18 should apply.

43 CNIL, *Annual Report 2003*, pp. 140 – 142. See also the webpage with results of the Internet poll referred to in the text: www.cnil.fr/index.php?id=1557.

44 Note that the term 'legitimate' here (and on the Continent in general) has a much wider meaning than 'lawful', to include the question of whether the matter is socially acceptable. For details, see the discussion in Chapter 7 of the *Children's Databases* report (footnote 1, above) of the terminology used in the British Data Protection Act.

45 *Biométrie: quatre refus d'autorisation d'utilisation des empreintes digitales:* CNIL, 30/01/06, on http://www.cnil.fr/index.php?id=1938&news[uid]=304&cHash=1b5bb06ad5.

46 *Advies Nr 38/2002 van 16 september 2002 betreffende de bescherming van de persoonlijke levenssfeer van minderjarigen op Internet/Avis N° 38/2002 du 16 septembre 2002 relatif à la protection de la vie privée des mineurs sur l'Internet* (Advice No. 38/2002 of 16 September 2002 concerning the protection of the private life of minors on the Internet). The full text can be found on the Privacy Commission's website at: http://www.privacycommission.be/nl/docs/Commission/2002/advies_38_2002.pdf (Dutch);
http://www.privacycommission.be/fr/docs/Commission/2002/avis_38_2002.pdf (French).

47 In the text, I deal first with the question of the age of maturity, and then with the data protection issues. In the Advice, the issue of legal age is dealt with within the broader data protection discussion.

48 The summary in the text somewhat focusses on the more general comments and guidance, rather than on matters that are more specific to the question of children and the Internet, or where this can clearly be done without distortion, applies the specific comments and guidance of the Privacy Commission to the broader issues.

49 The Advice here, in a footnote, refers to, and reflects the wording of, the Working Paper of the International Working Group on Data Protection in Telecommunications (the 'Berlin Privacy Group') on 'Childrens' Privacy On Line: The Role of Parental Consent', adopted at the IWGDPT's 31st meeting in Auckland (New Zealand), on 26/27 March 2002. This Working Paper is further discussed in section 3.

50 *Lei 67/98 – Lei da Protecção de Dados Pessoais* (Law 67/98 – Law on the Protection of Personal Data), full text at: http://www.cnpd.pt/bin/legis/nacional/LPD.pdf. See also more generally the website of the NDPC: http://www.cnpd.pt/index.asp.

51 This is partly because the data protection authority was only fully established in 2004 under a separate law, the Lei 43/2004 – *Lei da organização e funcionamento da CNPD* (Law 43/2004 – Law on the organisation and operation of the CNPD), full text at: http://www.cnpd.pt/bin/cnpd/Lei_43_2004.pdf.

52 The problematic situation of the processing of personal data on children in care, and the rather surprising decision to place the matter in the hands of the Freedom of Information Commission rather than the Data Protection Commission, is described in section 3 of the longer paper on the law in Portugal, submitted separately.

53 See the examples given in the box in the longer paper on Portugal, on p. 2.

54 *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*, usually referred to as the LOPD, but in this paper simply referred to as 'the Law'. For the quotes in this paper, I have used the unofficial English translation of the Law provided on the website of the Spanish Data Protection Authority: https://www.agpd.es/portalweb/canaldocumentacion/legislacion/estatal/index-ides-idphp.php.

55 *Real Decreto 1720/2007, de 21 de diciembre*. Both the official version in Spanish and the unofficial translation in English can again be found on the website mentioned in the previous footnote.

56 The Decree adds to these stipulations in the Law, a provision on data sharing in the public sector (Article 10(4)(c)), which allows this when:

– The processing of the data is for historical, statistical or scientific purposes;
– The personal data have been collected or drawn up by one public administration for the specific purpose of being sent to another;
– The communication is carried out in order to exercise identical powers or powers relating to the same matters.

This may appear rather vague, although in practice it will be quite strictly applied. More important, when it comes to the sharing of sensitive data, the Law is much more strict: the Decree reiterates that such data may only be processed (or shared) on the basis of the special provisions contained in Articles 7 and 8 of the Law, which hardly allow for any sharing of sensitive data without consent at all, with a very limited exception for the sharing of health data between the health care bodies belonging to the Spanish National Health Services, but even that is restricted to sharing 'for the purpose of medical care' (Article 10(5)).

57 There are separate authorities for Spain as a whole, the Basque Country, Catalonia, and Madrid.

58 See: http://www.bornsvilkar.dk/BornsVilkar.aspx. The page for children, with links to an advice phone and the chatroom is at: http://www.bornsvilkar.dk/ForBornOgUnge.aspx (I believe that *For Børn og Unge means For Children and Young People*).

Produced for ARCH by

The National Youth Agency

Getting it right for young people

Eastgate House, 19–23 Humberstone Road, Leicester LE5 3GJ.
Tel. 0116 242 7350. Fax: 0116 242 7444.
E-mail: nya@nya.org.uk
Websites: www.nya.org.uk www.youthinformation.com

Printed by Spectrum, Leicester.